



**UNIVERSIDAD NACIONAL DE INGENIERIA
RECINTO UNIVERSITARIO SIMON BOLIVAR
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

**TRABAJO MONOGRAFICO PARA OPTAR AL TITULO DE
INGENIERO EN ELECTRONICA**

**IMPLEMENTACION DEL PROTOCOLO SNMP PARA EL MONITOREO Y
CONTROL CENTRALIZADO DE LOS SISTEMAS DE COMUNICACIÓN,
NAVEGACION Y VIGILANCIA DE COCESNA A TRAVES DE LA APLICACIÓN
SOFTWARE SOLARWINDS.**

Autor:

Br. Aurora María Zeas Arias

Tutor:

Marco A. Munguía Mena, TeKnL

Managua, 31 de Enero del 2018.

Dedicatoria

A Dios todo poderoso por darme sabiduría y entendimiento para poder llegar a esta etapa de culminación de mis estudios de pregrado.

A mis padres Jerónimo Zeas y Alma Arias; a mi Abuela y familia. Gracias por el apoyo brindado durante mis estudios y a lo largo de toda mi vida.

Agradezco al ingeniero Marcos Zelaya, por darme la oportunidad de desarrollar mis conocimientos y a los ingenieros Javier Girón y Milton Zeledón por guiarme durante la realización de este proyecto.

Aurora Zeas

RESUMEN

El presente documento tiene como objetivo principal mostrar el procedimiento y los beneficios que se obtuvieron al implementar el monitoreo y control centralizado en la Corporación Centroamericana de Servicios de Navegación Aérea (COCESNA-Nicaragua), mediante el protocolo Simple de Gestión de Red (SNMP) y el software Solarwinds.

Se realizó una identificación de los equipos que están dentro de la plataforma TCP/IP de COCESNA que soportan el protocolo SNMP. Así mismo, se determinaron aquellos equipos pertenecientes a la red que no lo soportan. Posteriormente, se definieron los procedimientos para integrar cada equipo de la red en el software de gestión Solarwinds.

Una vez realizada la incorporación de todos los equipos, se procedió a ejecutar pruebas del funcionamiento del sistema de monitoreo de la red de comunicaciones, en donde se ajustaron los parámetros de funcionamiento para verificar que los diferentes componentes actuaban dentro de los requerimientos del sistema.

Con la implementación de este sistema, se obtuvieron datos en tiempo real del funcionamiento de los equipos monitoreados, lo que ha permitido reducir el tiempo de mantenimiento correctivo, con la posibilidad de analizar estadísticamente las causas del fallo y determinar los tiempos entre fallas. Con esta información se han tomado decisiones gerenciales importantes que reducen costos asociados al mantenimiento, tales como mantener un mínimo de repuestos en stock y optimizar el tiempo del personal de mantenimiento de los equipos. Adicionalmente, con el software Solarwinds se puede monitorear el funcionamiento de los equipos que posee COCESNA en la región centroamericana.

INDICE

RESUMEN	4
INDICE	1
1. INTRODUCCION.....	3
2. OBJETIVOS.....	5
2.1 OBJETIVO GENERAL	5
2.2 OBJETIVOS ESPECIFICOS.....	5
3. JUSTIFICACION	6
4. MARCO TEORICO.....	7
4.1 MONITOREO Y CONTROL	7
4.2 PROTOCOLO SNMP	8
4.2.1 MIBs.....	9
4.2.2 OPERACIONES SNMP	10
4.2.3 VERSIONES SNMP	13
4.3 DISPOSITIVOS NO SNMP	14
4.3.1 UNIDAD TERMINAL REMOTA (RTU)	14
4.4 SOLARWINDS	15
4.4.1 CARACTERISTICAS CLAVES DE SOLARWINDS	16
4.4.2 FUNCIONAMIENTO DE ORION PERFORMANCE NETWORK	19
5. IMPLEMENTACION DE SOLARWINDS NPM NETWORK PERFORMANCE MONITOR	21
5.1 LICENCIAS DE SOLARWINDS NPM.....	21
5.2 REQUERIMIENTOS DE SOLARWINDS NPM.....	22
6. COCESNA	23
6.1 SISTEMAS DE COMUNICACIÓN	23

6.2 SISTEMAS DE NAVEGACION	25
6.3 SISTEMAS DE VIGILANCIA	25
7. IDENTIFICACION DE EQUIPOS EN LA RED TCP/IP DE LA RED DE COCESNA Y LOS QUE NO PUEDEN SER GESTIONADOS A TRAVES DE SNMP	25
7.1 DISPOSITIVOS QUE SOPORTAN GESTION A TRAVES DE SNMP	26
7.2 GESTION DE DISPOSITIVOS NO SNMP	28
8. INTRODUCCION DE LOS DISPOSITIVOS GESTIONADOS EN SOLARWINDS....	31
9. EJECUCION DE PRUEBAS Y RESULTADOS	38
9.1 PRUEBAS DE OPERATIVIDAD EN DISPOSITIVOS GESTIONADOS A TRAVES DE SNMP	38
9.2 PRUEBAS DE OPERATIVIDAD EN DISPOSITIVOS NO SNMP GESTIONADOS ATRAVES DE UN AGENTE PROXY.....	46
10. CONCLUSIONES.....	50
11. RECOMENDACIONES	51
12. BIBLIOGRAFIA.....	52
13. ANEXOS	54

1. INTRODUCCION

COCESNA es un Organismo Internacional de Integración Centroamérica, sin fines de lucro y de servicio público, conformada con 6 estados miembros (Belice, El Salvador, Honduras, Nicaragua, Guatemala y Costa Rica) cuya sede principal se encuentra en Honduras; prestando servicios en las áreas de Navegación Aérea, Capacitación Aeronáutica y Seguridad Aeronáutica.

Entre los diferentes servicios que brinda COCESNA, se prioriza la seguridad aeronáutica. Se cuenta con equipos operativos para asegurar la calidad en los servicios brindados. La supervisión y control constante de los equipos es una labor de vital importancia para evitar que estos queden fuera de servicio. Además, de ser actividades costosas, resultan muy complicadas, ya que la mayoría de estos sistemas se encuentran instalados en diferentes sitios de Nicaragua y es necesario trasladar personal a estos sitios para conocer el estado de los sistemas y equipos.

El crecimiento acelerado y continuo de los diferentes dispositivos en la red de COCESNA, creó la necesidad de monitorear todos estos dispositivos. De tal manera, que permitiese al personal observar constantemente el estado de los equipos y obtener una solución rápida ante un fallo, mejorando los tiempos de respuesta. Dado que COCESNA carecía de un software de monitoreo centralizado que posibilitara la supervisión en tiempo real de los dispositivos, se decidió en este proyecto de finalización de carrera, desarrollar un sistema de monitoreo y control centralizado, mediante el protocolo Simple de Gestión de Red (SNMP) y el software Solarwinds.

Para mejorar la fiabilidad de los equipos que conforman los diferentes sistemas de seguridad aeronáutica, se aprovecharon las ventajas que brinda el protocolo SNMP y las características que el software SolarWinds ofrece, lo que permite tener un monitoreo centralizado, con la finalidad de prestar servicios con calidad y seguridad para los usuarios de la aviación civil. Reduciendo las sorpresas y pérdidas operativas, tomando mejores decisiones de respuesta a los riesgos

La implementación de este proyecto se realizó en conjunto con especialistas del área de Telecomunicaciones de COCESNA, quienes cuentan con el conocimiento en los sistemas a monitorear y además han desarrollado algunos proyectos con aplicaciones similares, pero sin las prestaciones que SolarWinds ofrece.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Realizar la implementación del protocolo SNMP con la aplicación Software “Solarwinds” para el monitoreo y control centralizado de los sistemas de comunicación, navegación y vigilancia en COCESNA

2.2 OBJETIVOS ESPECIFICOS

- Identificar los equipos que están dentro de la plataforma TCP/IP y los que no soportan el protocolo SNMP.
- Implementar el protocolo de gestión SNMP para monitorear y controlar los equipos de COCESNA.
- Definir parámetros específicos de las MIBs (Management Information Base), el cual dependerá del equipo gestionado.
- Integrar los equipos no SNMP a la plataforma de gestión SolarWinds mediante un equipo RTU (Remote Terminal Unit).
- Utilizar la herramienta de software SolarWinds como una plataforma centralizada para el monitoreo de los sistemas.
- Efectuar una serie de pruebas que permita la comprobación del buen funcionamiento del monitoreo.

3. JUSTIFICACION

Dado que la mayoría de los sistemas que COCESNA tiene instalados en distintas zonas del país, tenían la posibilidad de ser monitoreados a través de la red, COCESNA vio la necesidad y oportunidad de implementar un software que le permitiera obtener un monitoreo centralizado con el objetivo de controlar ciertas variables remotamente. De esta manera se obtendría resultados positivos tales como:

- 1- Mejora en el tiempo de respuesta a fallos
- 2- Anticipación de posibles fallos y evitar las fallas
- 3- Obtención de datos en tiempo real
- 4- Optimización de Recursos
- 5- Tener un mejor control de los sistemas, permitiendo obtener de manera automática bases de datos, gráficos, etc... de los eventos ocurridos en los sistemas para así predecir problemas y poder reducir la posibilidad de falla.

4. MARCO TEORICO

4.1 MONITOREO Y CONTROL

Actualmente las empresas le dan una gran importancia a la información y la forma en la que se maneja la red. El monitoreo de red y el procesamiento de datos, son funciones importantes que permite observar en tiempo real el comportamiento de los equipos conectados a la red.

El monitoreo de la red es un proceso eminentemente pasivo que se encarga de observar el estado y comportamiento de la configuración de red y sus componentes. También se encarga de agrupar todas las operaciones para la obtención de datos acerca del estado de los recursos de la red.

Las funciones del monitoreo de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad, realizan la detección de eventos y la comunicación de alertas.

El monitoreo de red abarca 4 fases:

- 1- Definición de la información que se monitorea
- 2- Acceso a la información
- 3- Diseño de políticas de administración
- 4- Procesamiento de la información

A diferencia del monitoreo, el control es un proceso que puede considerarse como activo, ya que permite tomar la información del monitoreo y actuar sobre el comportamiento de los componentes de la red administrada.

En forma general, lo que pretende el monitoreo y el control de red es minimizar los riesgos frente a una posible falla, minimizar el costo asociado con las operaciones, al evitar que suceda algún tipo de problema y mantener la red en funcionamiento brindando los servicios sin ningún problema.

4.2 PROTOCOLO SNMP

El SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de gestión entre dispositivos de una red. Permite a los administradores de red supervisar el rendimiento de la red, buscar y resolver sus problemas y planear el crecimiento de la red.

Una red administrada con SNMP consiste de tres componentes fundamentales [1]:

1. Dispositivos Administrados. (MD por sus siglas en ingles)
2. Agentes
3. Sistemas administrados por la Red. (NMS Por sus siglas en ingles)

Un MD, es un nodo de red que contiene un agente SNMP y que reside en una red administrada. Los MD recopilan y almacenan información y hacen que esta información esté disponible al NMS utilizando SNMP. Estos MD también llamados elementos de red pueden ser routers y servidores de acceso, switches y bridges, hubs, computadoras anfitrionas o impresoras.

Un agente es un módulo de un software de gestión de red que reside en un dispositivo administrado. Un agente tiene conocimiento local de información (capacidad de la memoria, número de paquetes recibidos y enviados, instrucciones IP, rutas, etc.) y traduce esa información a un formato compatible con el SNMP.

Un NMS ejecuta aplicaciones que monitorean y controlan Dispositivos Administrados. Proporcionan la mayor parte de recursos de procesamiento y memoria requeridos para la gestión de la red. En una red administrada existe al menos un NMS [1].

An SNMP-Managed Network Consists of Managed Devices, Agents, and NMSs

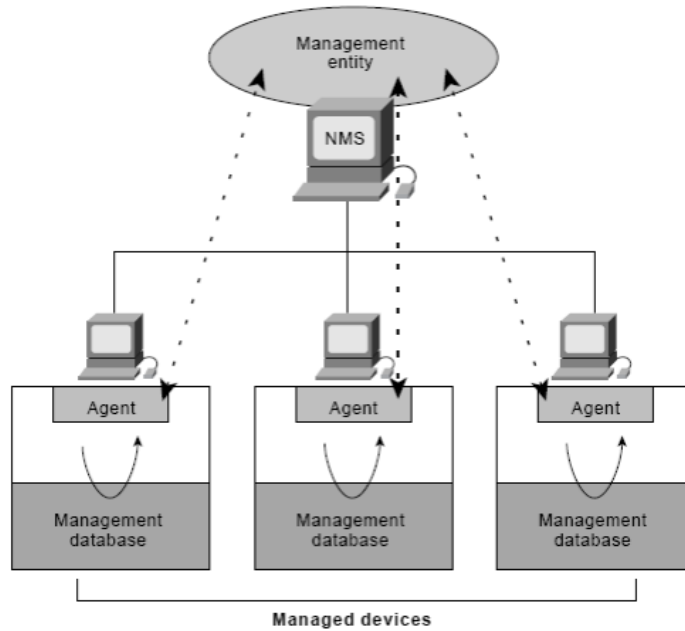


Figura 1. Ilustra la relación entre MD, Agent y NMS. Figura extraída de [1]

4.2.1 MIBs

La MIB es un área de almacenamiento de información virtual para la gestión de la red, que consta de colecciones de objetos gestionados.

Cada objeto guardado en una MIB tiene un identificador que lo identifica de manera única. Este identificador es conocido como el identificador de objeto (OID por sus siglas en ingles).

La MIB SNMP es organizada en una estructura de árbol con variables individuales [2]. Cada nodo del árbol tiene asociado un número entero y una etiqueta de texto. Un nodo se identifica unívocamente con una secuencia de números enteros que identifican los nodos a través de los cuales hay que pasar para llegar desde la raíz al nodo que interese [2].

El siguiente gráfico muestra parte del árbol definido por la Organización Internacional de Normalización (ISO por sus siglas en ingles), (véase figura.2):

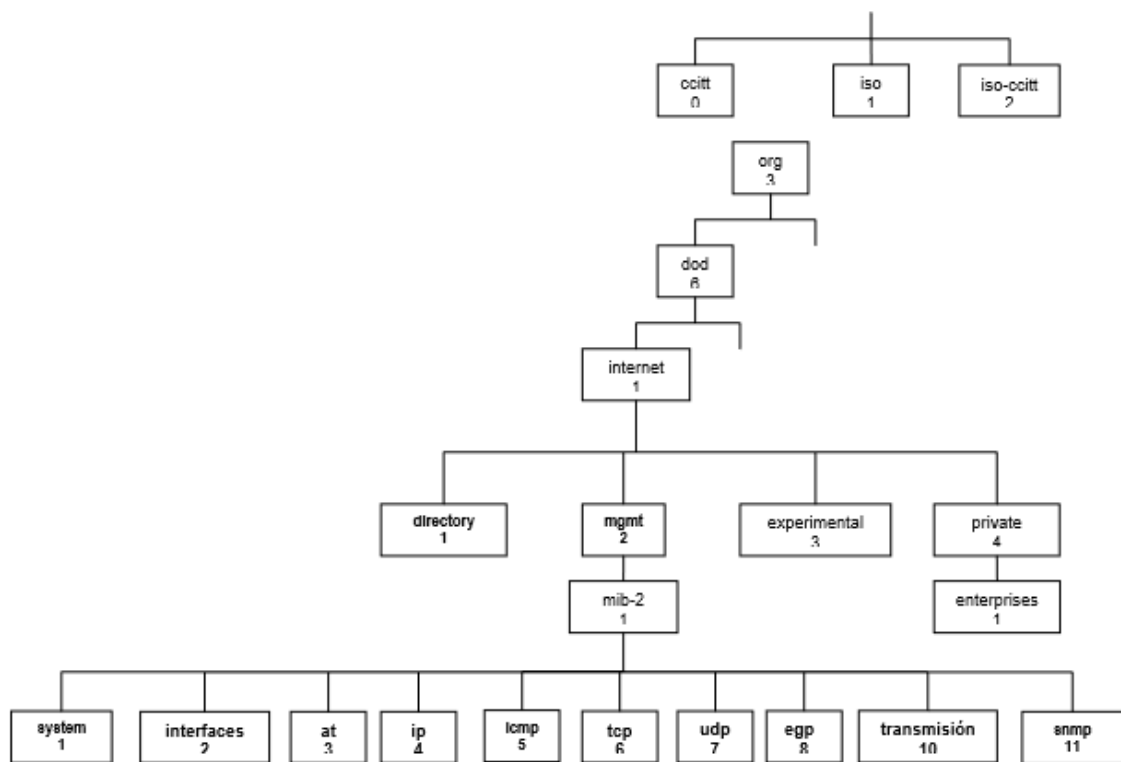


Figura 2: Estructura General de la MIB

La MIB se define utilizando la sintaxis ASN.1. y, es utilizada para describir las estructuras de datos que queremos definir para guardar la información de gestión. Luego de definir estas estructuras se debe definir la sintaxis de transferencia, para saber la forma en que van a ser transmitidos los datos en la red. A esto se le conoce como las reglas de codificación básicas (BER). Es la codificación utilizada para transferir información escrita en ASN.1 a otras aplicaciones mediante una sintaxis que permite definir el formato de cómo se van a enviar los datos.

4.2.2 OPERACIONES SNMP

SNMP es un protocolo simple de petición o solicitud / respuesta. El NMS emite una solicitud y los MD devuelven una respuesta. Este comportamiento se implementa

mediante el uso de una de las cuatro operaciones del protocolo: Get, GetNext, Set y Trap: [3].

- La operación Get es utilizada por el NMS para recuperar el valor de una o más instancias de un objeto desde un agente. Si el agente responde a la operación Get y no puede proporcionar valores para todas las instancias del objeto en una lista, no proporcionará entonces ningún valor.
- La operación GetNext es utilizada por el NMS para recuperar el valor de la siguiente instancia del objeto en una tabla o una lista dentro de un agente.
- La operación Set es usada por el NMS para colocar los valores de los objetos dentro de un agente.
- La operación Trap es utilizada por los agentes para informar asincrónicamente al NMS sobre un evento importante.

La versión SNMP V2 define 2 nuevas operaciones de protocolo: GetBulk e Inform

La operación GetBulk es utilizada por el NMS para recuperar de manera eficiente grandes bloques de datos, tales como múltiples filas de una tabla. La operación GetBulk llena un mensaje de respuesta con la mayor cantidad de datos solicitados.

La operación Inform permite que un NMS envíe Traps hacia otro NMS y luego reciba una respuesta

La mayoría de mensajes (Get, GetNext, y Set) son únicamente emitidos por el administrador SNMP, debido a que el mensaje TRAP es el único mensaje capaz de ser iniciado por un agente, y este es el mensaje utilizado por RTU (remote telemetry units) para informar de las alarmas

En la figura 3 se puede apreciar como es el proceso de intercambio de mensajes o más bien, PDUs (*unidades de protocolo de datos*) de SNMP para los comandos de Get, Set, Trap entre la consola, el administrador y el agente.

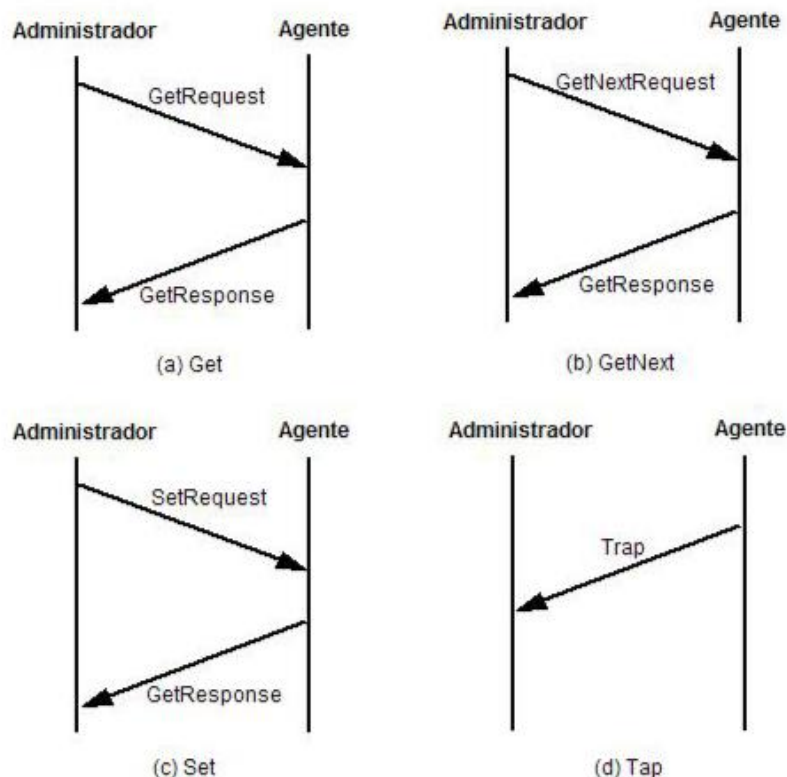


Figura 3: Intercambio de Mensajes SNMP

El agente responde a un mensaje `getrequest` con un comando `getresponse` el cual contiene el mismo ID de petición, un campo dentro del formato de un mensaje SNMP que contiene una identificación única para cada mensaje de solicitud (figura (3a)). El formato `getrequest` puede acceder a todas las variables solicitadas en el campo variable, entonces se puede generar una respuesta `getresponse` que contiene una lista de las variables con sus correspondientes valores.

De forma similar funciona el comando `getnextrequest` (figura 3 b), la diferencia radica en que esta va a retornar la siguiente instancia de un objeto.

El comando `setrequest` (fig 3 c) es muy similar a `get request`, pero la diferencia sustancial radica en que el fin de esta operación es el de escribir un valor y no el de leerlo. Por último, el comando `trap` (fig 3 d) no necesita recibir mensajes para mandar los datos. A diferencia de los comandos anteriores, este comando es generado por el agente cuando

en el dispositivo que monitorea sucede algo excepcional y debe ser notificado al administrador [4].

4.2.3 VERSIONES SNMP

SNMPv1- Es la administración más sencilla de red. Protocolo desarrollado para la gestión de los dispositivos sobre una red IP. [5]

SNMPv2- Es una evolución de SNMPv1. Presenta varias características que la versión 1 no satisfacía tales como:

- Mayor eficiencia en la transferencia de la información.
- Capacidad de los sistemas de operar tanto como agente como gestores.
- Soporta una señalización extendida de errores.
- Permite el uso de varios servicios de transporte. [6], [7], [8]

SNMPv3- Es un protocolo de interoperabilidad basado en estándares para la gestión de red. Esta versión provee las siguientes características de seguridad. [9], [10], [11]

- Autenticación: verifica que la solicitud proviene de una fuente genuina.
- Privacidad: con esto se refiere a la encriptación de datos.
- Autorización: verifica que el usuario permite la operación solicitada.
- Control de acceso: Comprobación de que el usuario tiene acceso a los objetos que se solicitan.

Vale la pena mencionar que las dos primeras versiones de SNMP son muy inseguras ya que no implementan ningún método de seguridad

En términos de seguridad las versiones SNMPv2c y SNMPv3 no son las más apropiadas por lo que se ha decidido trabajar en este proyecto con SNMPv3 por que posee un nivel de seguridad más alto (Utiliza Autenticación).

4.3 DISPOSITIVOS NO SNMP

SNMP se originó en la comunidad de internet como medida para administrar redes TCP/IP. Como no todos los dispositivos fueron creados con una mentalidad que pudiesen ser administrados mediante SNMP existen varios equipos que no pueden ser administrados con SNMP. Para esto existe un agente especial llamado proxy que permite administrar este tipo de dispositivos.

Básicamente actúa como un convertidor de protocolos que traduce de SNMP al esquema propio definido en el dispositivo. Este tipo de agente es muy útil para administrar dispositivos que son administrados por un esquema propietario y se desean incorporar al mundo SNMP.

Para dar un ejemplo de los dispositivos en los que se necesita ser de un agente-proxy, se encuentran; Generadores Eléctricos, UPS, Alarmas de Intrusión, Sensores del entorno (Humo, Temperatura, Humedad), Aires Acondicionados, etc.

4.3.1 UNIDAD TERMINAL REMOTA (RTU)

La RTU es la versión más avanzada de los PLC (control lógico programable), que sólo puede seguir una programación específica llamada lógica de escalera. Una RTU es sofisticada y suficientemente inteligente para controlar múltiples procesos sin requerir la intervención de un control maestro. Puede monitorear parámetros análogos y digitales a través de sensores así como datos provenientes de sistemas o equipos conectados; luego envía estos datos a la estación central de monitoreo. Son utilizadas en muchas instalaciones industriales (industrias de energía, petróleo y las instalaciones de distribución de agua). [4]

Una RTU incluye un software de configuración que conecta los flujos de entrada y salida de datos; El software puede definir protocolos e incluso solucionar problemas de instalación. Dependiendo del fabricante, del propósito y del modelo, una RTU puede ser expandible y ajustada con diferentes tarjetas de circuito incluyendo interfaces de

comunicación, almacenamiento adicional, alimentación adicional (power) y varias entradas analógicas y digitales I/O, así como interfaces para diferentes sistemas. [4]

Existen distintas marcas de RTU que se pueden encontrar fácilmente en el mercado, tales como: Siemens, ABB, wlink, DPS Telecom, Omniflex, Thermo Scientific, Schenider Electric, entre otras... COCESNA adquirió unidades del Fabricante DPS Telecom para el desarrollo del presente trabajo puede observarse en el anexo 1., con el propósito de incluir en el monitoreo todos los dispositivos que no tienen el medio de comunicación apropiado para la gestión SNMP. Entre ellos se encuentran: Generadores, UPS, Alarmas de intrusión, Alarmas contra incendio, Aires Acondicionados, incluyendo sensores del entorno

4.4 SOLARWINDS

SolarWinds es un software que ofrece una gestión completa del rendimiento de los fallos y de la red. Se puede ampliar al crecimiento acelerado de la red y se expande a las necesidades de supervisión de la red, permitiendo al usuario recopilar la información, ver la disponibilidad y las estadísticas en tiempos reales e históricos directamente desde su navegador web. Mientras supervisa, recopila y analiza datos de enrutadores, conmutadores, firewalls, servidores y otros dispositivos habilitados para SNMP, ICMP (Protocolo de Mensajes de Control de Internet) o WMI (en español, Instrumental de administración de Windows).

Este software proporciona una rápida visibilidad del estado de los dispositivos de la red, de los servidores y las aplicaciones de la red, asegurando que dispone de la información en tiempo real que necesita para mantener sus sistemas funcionando al máximo rendimiento. [12]

Las siguientes métricas críticas de rendimiento son monitoreadas por SolarWinds para dispositivos físicos y virtuales en la red:

- Disponibilidad de red

- Utilización de la capacidad de ancho de banda
- Uso de búfer y errores
- Utilización de CPU y memoria
- Errores de interfaz y descartes
- Latencia de red
- Nodo, interfaz y estado de volumen
- Uso de volumen

4.4.1 CARACTERISTICAS CLAVES DE SOLARWINDS

DESCUBRIMIENTO DE DISPOSITIVOS AUTOMATICOS Y PROGRAMADOS

Esta característica facilita la adición de dispositivos e interfaces a SolarWinds. Con solo responder a algunas preguntas generales sobre los dispositivos, la aplicación de descubrimiento se hace cargo, suministrando la información de inicio y comenzando de inmediato el análisis de red.

También le permite crear programas de descubrimiento de redes para ejecutar de forma independiente y automática. [12]

INTERFAZ DE MONITORIZACION

Ayuda a recopilar, analizar y visualizar los datos consultados para las interfaces supervisadas, así como la información sobre posibles desajustes dúplex o el tiempo de inactividad de la interfaz. [12]

NETWORKATLAS

Con Connect Now NetworkAtlas, la aplicación de mapeo de redes, permite crear mapas multi-capas, completamente personalizables por ejemplo ver anexo 2. Se puede rastrear visualmente el rendimiento de cualquier dispositivo en cualquier ubicación a través de la red, en tiempo real. Esta característica automáticamente drena enlaces entre los nodos

físicos directamente conectados descubiertos en su red usando datos de topología Layer2 y Layer3. [12]

INFORMES HISTORICOS DETALLADOS

Permite configurar fácilmente los informes de datos de la base de datos durante períodos de tiempo personalizados. Con más de 40 informes integrados disponibles, puede proyectar las tendencias futuras y las necesidades de capacidad, e inmediatamente acceder a las estadísticas de disponibilidad, rendimiento y utilización.

Mediante el WebReportScheduler, puede enviar por correo electrónico, imprimir o guardar informes de forma regular, directamente desde la consola web. [12]

UNPLUGGABLE-PORTMODE

Permite designar los puertos seleccionados como desconectables, por lo que las alertas innecesarias no se activan cuando los usuarios desacoplan o apagan los dispositivos conectados.

Esta característica es particularmente útil para distinguir en puertos de baja prioridad conectados a ordenadores portátiles y PC de puertos de infraestructura de mayor importancia crítica [12]

UNIVERSAL DEVICE POLLERS

Universal Device Poller permite fácilmente agregar cualquier dispositivo habilitado SNMP en la base de datos de monitoreo local y recolectar estadísticas o información que esta referenciada en la tabla MIB del dispositivo [12]

INTEGRATED TRAP AND SYSLOG SERVERS

SolarWinds permite ahorrar tiempo al investigar problemas de red, dando la posibilidad de usar traps y mensajes Syslog para acceder a la información de red desde una sola interfaz en lugar de requerir que consulte varias máquinas. Puede usar SolarWinds para configurar fácilmente alertas y luego recibir, procesar, reenviar y enviar mensajes syslog y trap. [12]

GROUPS AND DEPENDENCIES

La capacidad de definir grupos de dispositivos y dependencias le permite administrar más eficazmente la red. Los grupos le permiten organizar de forma lógica los objetos supervisados, independientemente del tipo o ubicación del dispositivo, y las dependencias le permiten representar más fielmente lo que realmente se puede saber acerca de la red monitoreada, eliminando los disparadores de alerta "falsos positivos" y proporcionando una visión más precisa del estado del objeto de red supervisado [12]

VMWARE INFRASTRUCTURE MONITORING

Monitorea los servidores, centros de datos y los clústeres de VM, incluyendo VMware ESX y ESXi, el Centro Virtual y cualquier máquina virtual (VM) alojada por servidores ESX en su red. [12]

INCIDENT ALERTING

Alertas totalmente personalizadas para dar repuesta a cientos de posibles escenarios de red. ayudando a reconocer los problemas antes de que los usuarios de la red experimenten impactos de productividad.

Los métodos y las respuestas de entrega de alertas incluyen correo electrónico, paginación, trampas SNMP, texto a voz, mensajería Syslog y ejecución de aplicaciones externas. [12]

CANAL NPM DE PRONÓSTICO

Proporciona información cuando la capacidad de sus nodos, interfaces y volúmenes se utilice completamente, ayudando a tomar las medidas apropiadas antes de que se produzcan problemas de uso completo

4.4.2 FUNCIONAMIENTO DE ORION PERFORMANCE NETWORK

A través de ICMP, SNMP, WM, comunicación Syslog y la recolección de datos NPM continuamente monitorea la salud y el comportamiento de la red, sin interferir con las funciones críticas de los dispositivos de la red

Luego de instalar Orion NPM, puede automatizar el descubrimiento inicial de la red y luego simplemente agregar nuevos dispositivos a medida que los agrega a su red. NPM almacena la información recolectada en una base de datos SQL (la base de datos SolarWinds) y proporcionan una consola web altamente personalizable y fácil de usar en la que puede observar el estado actual e histórico de la red [12]

El siguiente diagrama muestra un perfil de como SolarWinds monitorea la red. Ver Figura 4.

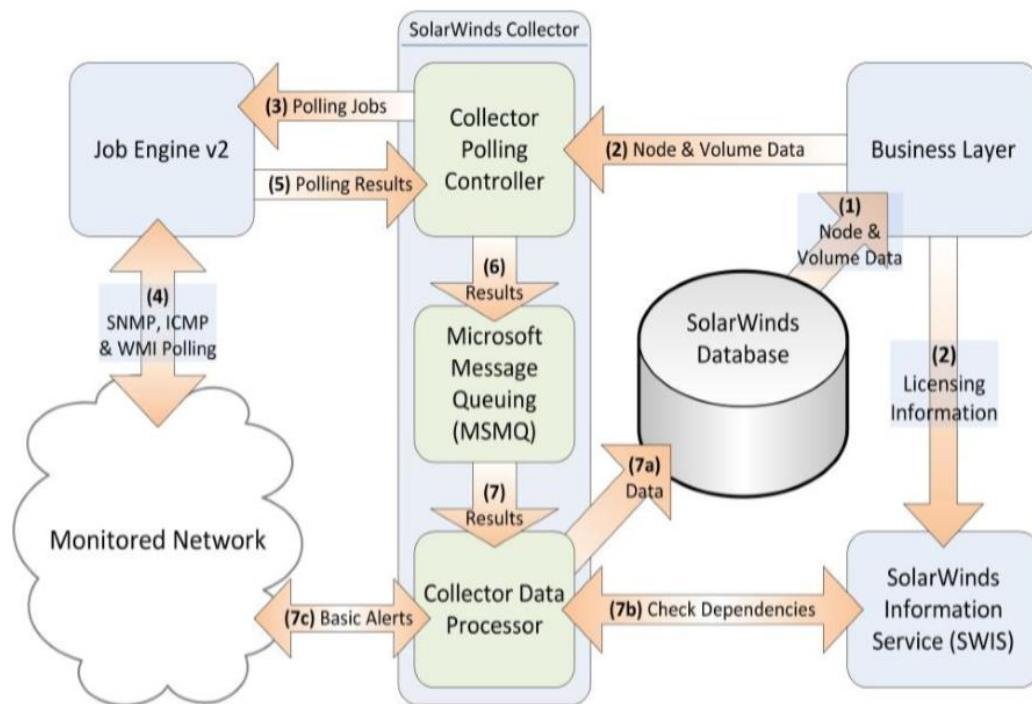


Figura 4: Perfil de monitoreo de Red mediante Solarwinds. Figura extraída de [12]

1. Después que “Network Sonar Discovery” ha poblado “the SolarWinds Database” con los objetos de red que se quieren monitorear, las informaciones de nodos y volúmenes son enviadas a la “Business Layer”.
2. “The Business Layer” pasa la información de nodos y volúmenes al “Collector Polling Controller” y provee información del tipo de licencia al “SolarWinds Information Service (SWIS)”.
3. El “Collector Polling Controller” crea los trabajos de polleo solicitados y los manda al “Job Engine v2”
4. “The Job Engine v2” realiza los trabajos de polleo solicitados, usando SNMP, ICMP y WMI, según hayan sido configurados en el “Network Sonar Discovery.”
5. “The Job Engine v2” luego pasa los resultados de todos los polleos solicitados al “Collector Polling Controller.”

6. “The Collector Polling Controller” ubica toso los resultados en el “Microsoft Message Queue (MSMQ).”
7. The Collector Data Processor extrae los resultados del MSMQ, y luego realiza las siguientes operaciones:
 - 7.a. The Collector Data Processor realiza cualquier calculo solicitado y luego inserta esos datos procesados en la base de datos de SolarWinds.
 - 7.b. The Collector Data Processor revisa con el (SWIS) si existe alguna dependencia definida en los nodos gestionados.
 - 7.c. The Collector Data Processor verifica el resultado del polling results Contra definiciones de alertas básicas existentes para determinar si se deben activar alertas básicas y acciones correspondientes.[12]

5. IMPLEMENTACION DE SOLARWINDS NPM NETWORK PERFORMANCE MONITOR

5.1 LICENCIAS DE SOLARWINDS NPM

Solarwinds NPM puede recolectar datos e información detallada de cualquiera de sus dispositivos habilitados para SNMP de versión 3 o versiones anteriores, incluyendo enrutadores, conmutadores, firewalls y servidores.

Solarwinds NPM se licencia de acuerdo al mayor número de los tres tipos de elementos de red supervisados:

1. **Nodos:** Los nodos incluyen dispositivos enteros, por ejemplo, enrutadores, conmutadores, servidores virtuales y físicos, puntos de acceso y módems.

2. **Interfaces:** Las interfaces incluyen puertos de conmutación, interfaces físicas, interfaces virtuales, subinterfaces, VLAN y cualquier otro punto único del tráfico de red.
3. **Volumenes** Los volúmenes son equivalentes a los discos lógicos que está supervisando

Existen niveles de licencias NPM las cuales se detallaran a continuación. Estos niveles van en dependencia de las necesidades que tenga el usuario.

1. Licencia SL100 permite monitorear hasta 100 nodos, 100 interfaces y 100 volúmenes (300 elementos en total).
2. Licencia SL250 permite monitorear hasta 250 nodos, 250 interfaces, and 250 volúmenes (750 elementos en total).
3. Licencia SL500 permite monitorear hasta 500 nodos, 500 interfaces, and 500 volúmenes (1500 elementos in total).
4. Licencia SL2000 permite monitorear hasta 2000 nodos, 2000 interfaces, and 2000 volúmenes (6000 elementos in total).
5. licencia SLX permite monitorear ilimitadamente elementos en la red [12]

5.2 REQUERIMIENTOS DE SOLARWINDS NPM

Tabla 1: Requisitos y Recomendaciones para Instalar solarWinds

Requisitos para instalar Solarwinds	Solarwinds Se puede instalar en
Servidor de sondeo de solarwinds que utiliza 4 nucleos de 3.0 Ghz o superior	Microsoft Windows server 2003 sp2 que incluye R2 (32 o 64 bits)
Procesamiento 8 GB RAM	Windows server 2008 R2 y R2 Sp1

Windows 2008 R2 Server (64 bit) con IIS Instalado, que funciona en modo de 32 bits	Windows server 2012
Microsoft. NET 3.5 SP1 y NET 4.0	

Para el servidor de base de datos de NPM puede instalar:

- Microsoft SQL server 2005 Express, standard o Enterprise,
- Sql server 2008 y 2008 R2 Express, standard o Enterprise
- Sql server 2012 Express, standard o Enterprise [12]

6. COCESNA

6.1 SISTEMAS DE COMUNICACIÓN

En la Región de Centroamericana COCESNA se dispone de una red de Telecomunicaciones heterogénea como se puede observar en la fig.5, compuesta principalmente de tres plataformas de comunicaciones que permite establecer dos tipos de subredes, la subred de Comunicaciones Aeronáuticas (SCA) y la subred de Comunicaciones Administrativas (SAD):

- **RED RTVS**, red de telecomunicaciones vía satélite diseñada en base al protocolo de comunicación Frame Relay enlazadas a través de una serie de estaciones VSAT, proporcionando una capacidad de comunicación de voz y datos en una red de conmutación de paquetes.
- **RED MICROONDAS**, está constituido por enlaces fronterizos, enlaces nacionales y enlaces de última milla. El sistema está compuesto por múltiples nodos que forman la columna vertebral para las transmisiones de voz/datos internacionales. La tecnología utilizada en esta red es vanguardista con un ancho de banda de 40 Mbps, escalable y con un esquema de protección; MHSB, diversidad completa y diversidad Híbrida. Los equipos pueden operar con modulaciones que van desde

QPSK, 16QAM y 128QAM ocupando anchos de bandas de 7 MHz, 14 MHz y 28 MHz respectivamente. Las bandas en las cuales operan estos enlaces son 6 GHz, 7 GHz, 8 GHz y 13 GHz con configuraciones 1+1.

- **RED DE ACCESO**, plataforma de enrutadores y switches de última generación que provee una infraestructura IP para el enrutamiento y entrega de los servicios sin obstrucciones ni dificultades. Para ello, la voz y el tráfico de datos están priorizados de forma diferenciada sobre la red, para acomodarse a la extra sensibilidad de las comunicaciones orales en consideración a los retardos, jitter, perdidas de paquetes, seguridad e incompatibilidad, que pueden afectar la calidad de los servicios de comunicaciones.

Estas redes permiten realizar los enlaces entre los países de Centroamérica: Honduras, Guatemala, Belice, El Salvador, Nicaragua y Costa Rica.

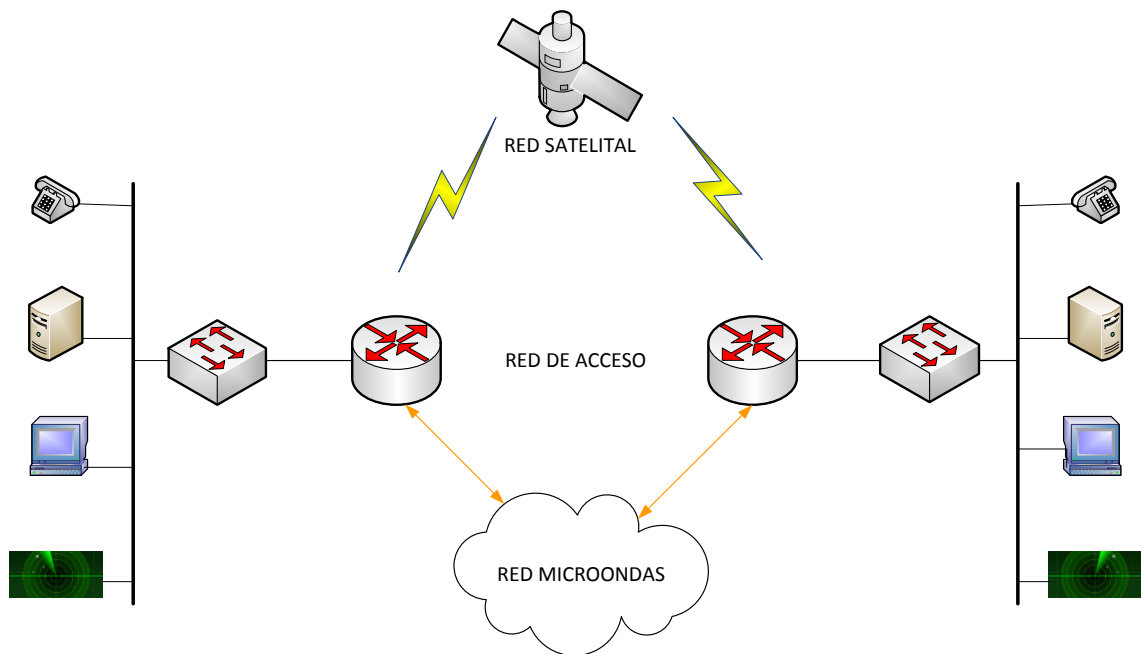


Figura 5: Red Heterogénea de COCESNA

6.2 SISTEMAS DE NAVEGACION

En los sistemas de Navegacion aeronáutica se conoce como “Radioayuda” al conjunto de señales radioeléctricas, generalmente generadas en instalaciones terrestres y recibidas a bordo, que permiten a la aeronave guiarse. Los sistemas que COCESNA tiene instalados se encuentran ubicados en distintas zonas del País, todos ellos están ubicados estratégicamente. A continuación se listan los principales sistemas de navegación:

- ✓ Rango Omnidireccional de Muy Alta Frecuencia empleando el principio Doppler (DVOR por sus siglas en ingles)
- ✓ Equipo de Medición de Distancia (DME por sus siglas en ingles)
- ✓ Rango Omnidireccional de Muy Alta Frecuencia (VOR por sus siglas en ingles)

6.3 SISTEMAS DE VIGILANCIA

Actualmente COCESNA tiene implementado un Radar secundario ubicado en Puerto Cabezas. Los radares secundarios de vigilancia se emplean en la navegación aérea civil para el apoyo al control del tráfico aéreo.

Los radares secundarios aumentan las condiciones de seguridad de los vuelos. Indican altitud, cómo está el cielo, la mejor ruta por la que debe irse en caso de que se presente algún problema como la erupción volcánica, y, de esta forma, que desde tierra te den mayores indicaciones.

7. IDENTIFICACION DE EQUIPOS EN LA RED TCP/IP DE LA RED DE COCESNA Y LOS QUE NO PUEDEN SER GESTIONADOS A TRAVES DE SNMP

Para realizar la identificación de los equipos que podían ser gestionados a través del protocolo SNMP en la red, se procedió, en conjunto con los ingenieros especialistas de la empresa, a revisar inventario de los equipos, modelos y características principales. De igual manera, se hicieron visitas de campo para identificar las condiciones propias del

lugar y aprovechar de mejor manera el monitoreo remoto; ya que estos sistemas se encuentran ubicados en distintas zonas del país por lo que las condiciones no son siempre las mismas.

Por motivo Seguridad de la empresa se mencionaran algunos de los equipos inventariados. Estos equipos que se van a detallar a continuación se repiten para cada uno de los sistemas CNS implementados en Nicaragua. En algunos casos pueden variar sus características, esto es por las condiciones propias del lugar


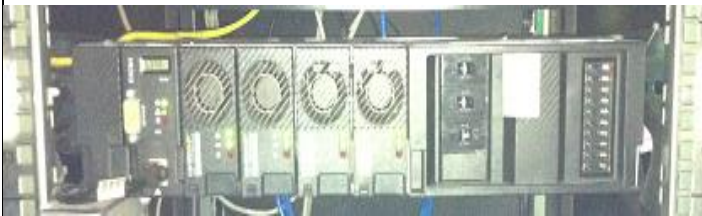

7.1 DISPOSITIVOS QUE SOPORTAN GESTION A TRAVES DE SNMP

Los dispositivos que pueden ser gestionados a través de SNMP, se caracterizan por poseer un módulo agente, base de datos de la información de gestión o MIB y una interface de red (generalmente Ethernet) que se comuniquen por el protocolo SNMP.

La red de COCESNA consiste de varios nodos por ejemplo, Puerto Cabezas, TWR Managua, Las Nubes, La Cuesta, La Casita. Por lo que es común que en cada nodo se encuentren réplicas de la infraestructura. Por tal motivo se procederá a dar una clasificación general de los equipos que se encontraron. Los cuales se puede ver en la tabla 2.

Tabla 2. Identificación de equipos que pueden ser gestionados mediante SNMP

Equipo	Ejemplo	Descripcion
Equipos de Radiocomunicación	 <p>Radio enlace Winlink-1000 1+1</p>	<p>Ubicado en la cabecera radar de Puerto Cabezas.</p> <p>Transmite datos radar, datos AIS, datos ATIS y canal de VOZ</p>

		hacia la torre de control
Equipos de enrutamiento	 <p>Router Cisco 2821</p>	Ubicado en Managua. Actúa como núcleo para la conmutación de los servicios a través de la red satelital y de microondas.
Equipos para el sistema de potencia	 <p>Rectificador marca ARGUS 1</p>	Ubicados en todos los nodos de la red AVIAT (Managua, TWR Managua, Las Nubes, La Cuesta, La Casita) para energizar los equipos de comunicaciones (-48 VDC).
Equipos para el monitoreo de Radionavegación	 <p>Monitor RCSE 443 ILS/DME: THALES (RCSE 443)</p>	Ubicado en torre de control de Puerto Cabezas. Ayuda a monitorear los equipos de navegación.

7.2 GESTION DE DISPOSITIVOS NO SNMP

Cuando se desea administrar información de un dispositivo que no soporta el protocolo SNMP, se requiere de un agente externo denominado “Agente Proxy” que sirva como Gateway de nuestra comunicación SNMP. Por lo general se trata de una terminal remota (RTU) que actuara como un sistema telemétrico que funciona por medio de transductores.

Al momento de empezar este trabajo monográfico COCESNA ya contaba con un equipo del Fabricante DPS TELECOM con el que esperaban dar solución, por lo cual se siguió trabajando con este (se puede trabajar con cualquier otro fabricante). Para recoger la información requerida se levantó un listado de los parámetros a ser monitoreados y así hacer toda una logística para la implementación del sistema telemétrico. De igual manera COCESNA ya contaba con un radioenlace. Por este motivo no es objeto de este proyecto realizar un radioenlace.

En el panel de alarmas de las condiciones del entorno se han instalados accesorios que facilitan el mantenimiento y conexión a los equipos. Por ejemplo; un Switch POE para la conectividad de red TCP/IP al Agente Proxy y un convertidor Serie/Ethernet para la administración del sistema ILS. El anexo 3 muestra la interconexión de todos estos dispositivos en el panel de alarmas.

Listado de parámetros en sitio Localizador Managua:

DE ALARMAS

- SENSAR LA ENERGIA COMERCIAL
- SENSAR LA ENERGIA DE RESPALDO
- ESTADO DEL GRUPO ELECTROGENO
- DETECCION DE INCENDIO
- DETECCION DE INTRUSO

DE CONTROL

- ARRANQUE DEL GRUPO ELECTROGENO
- PRUEBA DE RESPALDO DE GRUPO ELECTROGENO

ANALOGOS

- VOLTAGE DEL BANCO DE BATERIAS #1
- VOLTAGE DEL BANCO DE BATERIAS #2

SENSORES

- TEMPERATURA
- HUMEDAD RELATIVA

Todos los sistemas tienen características similares permitiendo generalizar el listado de parámetros, por esa misma razón se ha tomado de ejemplo el sistema ubicado en el Aeropuerto Augusto Cesar Sandino, Managua.

El RTU seleccionado para monitorizar todas estas variables es el modelo NetGuardian DIN que dispone de las siguientes características:

Hasta 8 entradas de alarma discretas

Hasta 8 análogos

1 toma de entrada del sensor D-Wire, admite hasta 32 sensores

6 salidas de relé de control

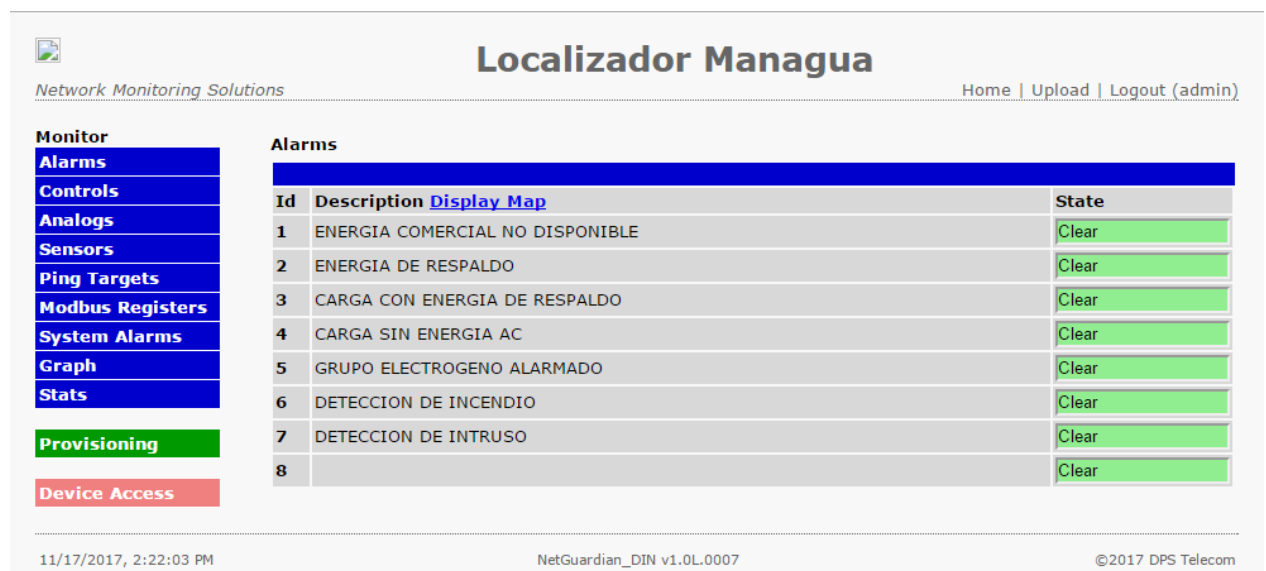
32 objetivos ping para monitorear otros dispositivos en la red. En el anexo 4 se detalla mayor información sobre este modelo.

Los transductores utilizados fueron los siguientes; Sensor de humedad, sensor de temperatura, sensor de humo y Relays. Estos transductores trabajan con señales de 4 a

20 mA, 0 a 5VDC y/o señales de contacto seco. Se efectuó la instalación de los equipos y cableados al sistema telemétrico.

En la configuración se definen los niveles de alarmas y las notificaciones SNMP para el gestor Solarwinds. Además, el RTU cuenta con su propio servidor WEB para la visualización de las señales medidas

En la figura 6 se muestra como es la visualización de las alarmas en el servidor web del net guardian Din. Todas las alarmas se encuentran en estado normal por lo cual están en color verde.



Localizador Managua

Network Monitoring Solutions Home | Upload | Logout (admin)

Monitor

- Alarms
- Controls
- Analogs
- Sensors
- Ping Targets
- Modbus Registers
- System Alarms
- Graph
- Stats

Provisioning

Device Access

Alarms

Id	Description Display Map	State
1	ENERGIA COMERCIAL NO DISPONIBLE	Clear
2	ENERGIA DE RESPALDO	Clear
3	CARGA CON ENERGIA DE RESPALDO	Clear
4	CARGA SIN ENERGIA AC	Clear
5	GRUPO ELECTROGENO ALARMADO	Clear
6	DETECCION DE INCENDIO	Clear
7	DETECCION DE INTRUSO	Clear
8		Clear

11/17/2017, 2:22:03 PM NetGuardian_DIN v1.0L.0007 ©2017 DPS Telecom

Figura 6. Estado de las alarmas

En los anexos 5 y 6 se presentan capturas de pantallas de cómo se observan las opciones de control, las mediciones de los niveles de las señales análogas, y las unidades de medidas según el tipo de sensor.

Al igual que en los dispositivos gestionados a través de SNMP Cada una de estas variables tienen la opción de poder configurarse para remitir un mensaje vía SNMP en caso de alguna anomalía a cada una de las personas responsables del área afectada.

Por ejemplo si el problema es meramente de energía, se enviara un Trap SNMP al correo de la persona responsable del grupo eléctrico.

8. INTRODUCCION DE LOS DISPOSITIVOS GESTIONADOS EN SOLARWINDS

Luego de haber definido las características más importantes de los dispositivos a monitorear y las condiciones de salida a los dispositivos que lo requieran en respuesta a algún fallo. Ahora se detallaran los recursos y pasos necesarios para la introducción de un dispositivo a Solarwinds.

Por la cantidad de dispositivos que se requieren monitorear en la estación de Nicaragua, COCESNA ha adquirido la licencia SL250 la cual permite monitorear hasta 250 nodos, 250 interfaces y 250 volúmenes siendo un total máximo de 750 elementos. Actualmente están siendo gestionados un total de 122 nodos, 172 volúmenes y 194 interfaces. Ver anexo 7.

Las características de software como de hardware utilizado para la instalación de solarwinds puede observarse en la tabla 3.

Tabla 3. Software y Hardware utilizados en COCESNA

HARDWARE	OS SOFTWARE
HP Proliant ML310e Gen8 Server, Torre de 4U, 4 slots PCIe x4(2) x8(1) x16(1) Procesador 4 core Intel® Xeon® E3-1220 V2 (8M cache, 3.10 GHz) Memoria RAM DDR3 4.0 GB Disco Rígido 1 Terabyte Monitor LG 32"	Windows Server 2008 R2 Standard Sistema Operativo 64-bit

Después de conocer los recursos que se ocuparon se mostrara un ejemplo de cómo se ingresan los dispositivos a gestionar en el software solarwinds para comenzar a ser monitoreados a través de la red. En este ejemplo se ingresara un Switch Cisco Catalyst 2960.

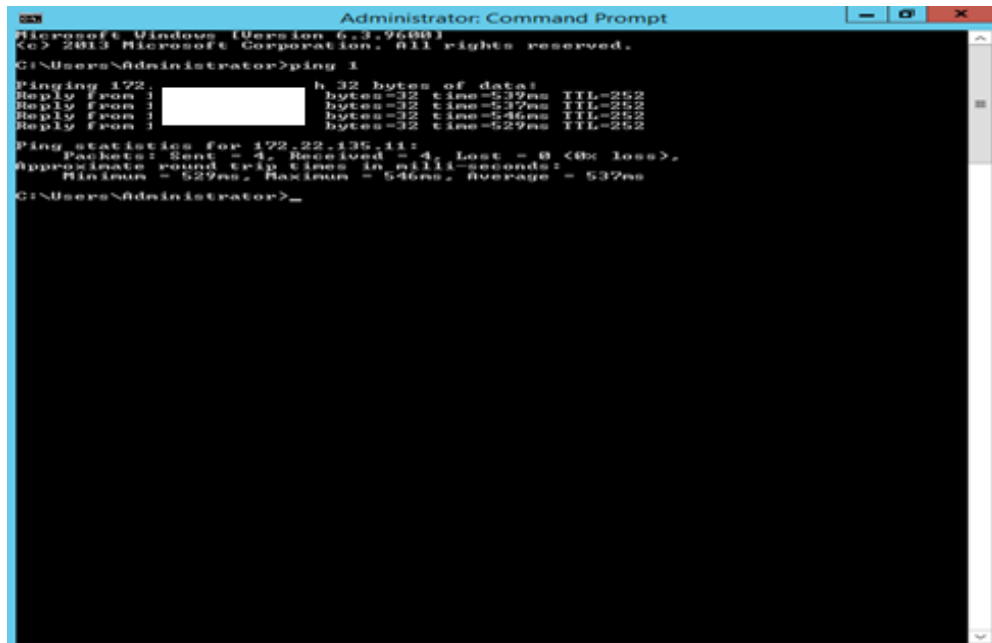
NOTA: Por motivo de seguridad y de políticas de COCESNA se ocultaran las direcciones IP.

Identificación de MIBS

Primeramente, se localiza la base de información de gestión o MIB-II del agente (dispositivo que se quiere gestionar), para luego sea compilado por el programa gestor en un formato legible y poder integrarlo. Para nuestro caso el NPM de SolarWinds posee una base de datos de la información de todos los fabricantes de dispositivos por lo cual nos ahorramos este paso y se puede agregar el elemento con la información básica tales como; memoria, CPU, temperatura, descripción del sistema, etc... Pero con otras plataformas se deberá localizar las MIB's con las que se quiere gestionar el equipo y estos se pueden conseguir generalmente en la página de internet del fabricante o bien se solicita al soporte técnico y se proveerá de manera gratuita. Sin embargo, los objetos a ser gestionados pueden ser varios y es necesario saber el OID para realizar el "polling" deseado. Es preciso tener conocimiento de algunas características del dispositivo tales como; el modelo y la versión del sistema ya que si no se usa el indicado se pueden recibir los Traps, Informes o Get Response de manera erróneos en el servidor.

Prueba de conectividad

El siguiente paso será de establecer la conexión remota con el dispositivo a través de una interfaz Ethernet del servidor y comprobar la conectividad por medio de la utilidad PING (Packet Internet Groper, Agrupador de Paquetes en Internet) ver fig 7. desde la consola DOS de Windows, si se recibe la respuesta significa que el dispositivo puede ser alcanzado desde el gestor (Network Performance Monitor) entonces procedemos a crear un nodo físico dentro de la topología de red y a este se le configurara un perfil SNMP en la opción para agregar un nuevo nodo, además de parámetros de utilidad.



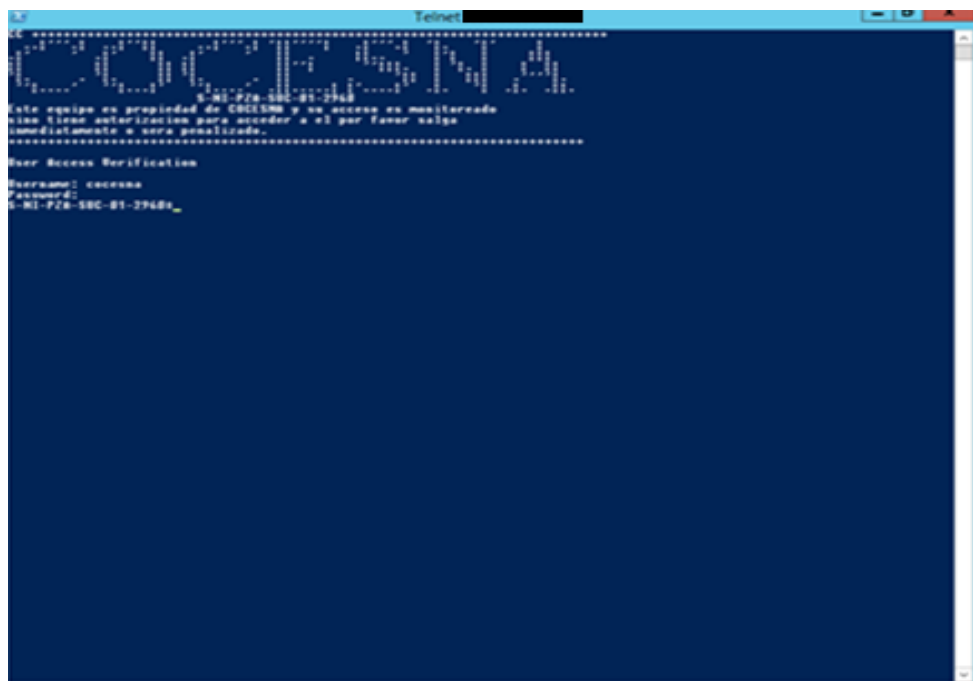
```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ping 1

Pinging 172.22.135.11: h=32 bytes of data:
Reply from 172.22.135.11: bytes=32 time=539ms TTL=255
Reply from 172.22.135.11: bytes=32 time=537ms TTL=255
Reply from 172.22.135.11: bytes=32 time=546ms TTL=255
Reply from 172.22.135.11: bytes=32 time=529ms TTL=255

Ping statistics for 172.22.135.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 529ms, Maximum = 546ms, Average = 539ms
C:\Users\Administrator>
```

Figura 7. Prueba de conectividad

Realizar Sesión telnetTelnet es un protocolo que sirve para emular una terminal remota.



```
Telnet
.....
CISCO
.....
Este equipo es propiedad de CISCOSM y su acceso es monitoreado
Solo tiene autorización para acceder a él por favor salir
inmediatamente o sera penalizado.
.....
User Access Verification
Username: cisco
Password: C-M-P/28-SBC-01-3948a_
```

Figura 8. Sesión Telnet

Una vez conectado al equipo remoto, se le solicitará que introduzca un nombre de usuario y una contraseña por razones de seguridad para permitir el acceso únicamente a los individuos autorizados. De hecho, la razón por la que Telnet es un protocolo tan potente es el hecho de que permite que los comandos se ejecuten en forma remota. El administrador de red define los comandos que son posibles ejecutar en una sesión Telnet.

Por tema de privacidad se Configurara el equipo Cisco switch catalyst 2960 con SNMPv3 [17]

* Para mejor visualización se presenta la Configuración en texto

snmp-server user cocesna grupoNI v3 auth sha Cocesna2000 priv des SolarWinds	Configura el grupo de servidores SNMP para habilitar la autenticación para los miembros de una lista de acceso específica especificada.
snmp-server group grupoNI v3 auth match exact read v3ro snmp-server group grupoNI v3 priv match exact write v3rw	estas comunidades se usarán cuando realice encuestas SNMP o edite en el dispositivo usando SNMPv3
snmp-server view v3ro mib-2 included	
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart	Habilita el envío de notificaciones SNMP Autenticación Controla el envío de

	<p>notificaciones de falla de autenticación SNMP.</p> <p>notificaciones de linkUp. Un Trap linkUp (3) significa que el dispositivo que envía reconoce que uno de los enlaces de comunicación representados en la configuración del agente ha surgido.</p> <p>Notificaciones linkDown (2) significa que el dispositivo emisor reconoce una falla en uno de los enlaces de comunicación representados en la configuración del agente.</p> <p>Un Trap coldStart (0) significa que el dispositivo de envío se está reiniciando a sí mismo de modo que la configuración del agente puede ser alterada.</p> <p>Una trap warmStart (1) significa que el dispositivo de envío se está reiniciando de forma tal que ni la configuración del agente ni la implementación de la entidad de protocolo están alteradas.</p>
snmp-server enable traps envmon	Habilita todas las notificaciones de SNMP disponibles en su sistema.

snmp-server host x.x.x version 3 priv cocesna	Especifica el destinatario de una operación de notificación de SNMP.
snmp-server trap-source vlan300	Especifica la interfaz VLAN de la dirección fuente del trap contenido en SNMP v1

En el anexo 8 se presenta los datos más relevantes para realizar una configuración SNMP. Luego de haber configurado el dispositivo que se quiere monitorear se procede a ingresarlo a la gestión de SolarWinds. Cualquier dispositivo que se quiera integrar deberá seguir los siguientes pasos:

1. Inicie sesión en el servidor de Orion NPM que aloja su instalación de Orion APM.
2. Haga clic en Orion Web Console en el grupo de programas de SolarWinds Orion.
3. Inicie sesión en Orion Web Console como administrador.
4. Haga clic en Admin (Administrador) en la barra de herramientas Views (Vistas).
5. Haga clic en Add a Node (Agregar un nodo) en la agrupación Node management (Gestión de nodos). Ver anexo 9.
6. Una vez agregado el nodo se configurara el nodo. Para ello se proporciona el nombre de anfitrión o la dirección IP del dispositivo que se desea agregar en el campo "Hostname" o "IP Address" (Dirección IP o nombre de anfitrión).
7. Como se mencionó anteriormente, se ha configurado el equipo con la versión 3 de SNMP por lo que ha seleccionado SNMPv3. El puerto utilizado por defecto es el 161 en caso de no estar predeterminado, proporcionar el número 161 en el campo "SNMP Port" ver anexo 10.

Si el nodo agregado es compatible con contadores de 64 bits y desea utilizarlos, marque "Allow 64 bit counters".

8. Proporcione la siguiente configuración de Credenciales SNMP, Autenticación y (Privacidad/Cifrado): Haga click en next ver anexo 11
9. Se elige el recurso a supervisar. Ver anexo 12. Haga click en next para visualizar la pestaña Add pollers. En esta pestaña se puede observar que la aplicación NPM contiene algunos pollers predefinidos para facilitar la información gestionada, entre ellas se encuentran; porcentaje de carga de la cpu, porcentaje de uso de memoria, voltajes de la fuente de alimentación, tablas de enrutamiento, etc... ver anexo 13
10. Luego de seleccionar lo que desea haga click en next, y por último "ok, add node".

Se puede observar como el nodo ha sido exitosamente agregado anexo 14

Como se ha agregado un nodo a Puerto Cabezas, se procede a verificar que realmente fue exitoso. Se puede visualizar todos los nodos ubicados en el departamento de Puerto Cabezas, al igual que los demás nodos anteriormente agregados de los distintos departamentos. Ver anexos 15, 16, 17

Seleccionamos el nodo que acabamos de agregar para observar a detalle información que está gestionando, la cual podemos editar según a nuestra conveniencia.

Hemos dado la opción de editar Top CPUs by percent load

La ventana que se nos abre, da la opción de cambiar el título, periodos de tiempo (aquí se puede seleccionar el rango de tiempo que queremos que muestre la información, cantidad de datos históricos, intervalos de tiempo)

Haga click en submit ver anexo 18.

Como se ha añadido un nodo recientemente podemos observar que no ha pasado el tiempo necesario para recopilar información, lo cual no nos permite obtener un gráfico de datos históricos. Ver anexo 19.

La configuración para integrar de los dispositivos NO SNMP, es exactamente el mismo procedimiento que acabamos de ver en el cual se integró un switch Cisco, la diferencia principal es que no se integra el dispositivo a ser gestionado, sino que se integra el RTU o el agente Proxy, en este caso sería el netguardian Din el cual se comunica vía SNMP al solarwinds.

En los anexos 20, 21 se puede observar cómo están conectados los diferentes sitios de COCESNA en donde tiene instalados sistemas de comunicación y navegación y Vigilancia con la estación central ubicada en Managua, km 10 ½ carretera Norte. Se ha hecho un zoom al mapa para observar la ubicación de los sistemas que se encuentran en el Aeropuerto Internacional Augusto Cesar Sandino como se puede observar en el anexo 22.

9. EJECUCION DE PRUEBAS Y RESULTADOS

9.1 PRUEBAS DE OPERATIVIDAD EN DISPOSITIVOS GESTIONADOS A TRAVES DE SNMP

Para comprobar la llegada de las notificaciones (Traps) al servidor se puede simular un fallo en el dispositivo, en caso de que el dispositivo se encuentre en servicio y no se pueda realizar la interrupción entonces convendría provocar un evento que no afecte los servicios como por ejemplo; la revisión de la configuración con el comando # show running configuration.

Para realizar la demostración se seleccionara un elemento gestionado de la red y se provocara una desconexión en una o varias de sus interfaces simulando un fallo en el puerto, además de otras acciones que provoquen un evento. Cuando se presenten las notificaciones en el gestor se analizarán las descripciones de los eventos transcurridos para la identificación de los sucesos. De esta forma podemos tomar las acciones pertinentes debido a la criticidad, tal como él envió de correo electrónico, mensaje sms, alarma audible, etc... al grupo, o persona responsable del sistema.

La configuración del Syslog en el dispositivo ayudara en la identificación de las notificaciones entrantes. Otras variantes se pueden configurar en el gestor para facilitar la supervisión y control de los dispositivos a continuación se mencionaran algunos:

Resolución DNS (Domain Name System, Sistema de Nombres de Dominio), con un servidor DNS en la red se podrá facilitar la identificación del dispositivo a través de nombres específicos.

Filtrado de Notificaciones, no todos los eventos son de extrema relevancia y pueden ofuscar las demás en la supervisión, para evitar la entrada de dichas notificaciones se puede realizar un filtrado dejando solamente las de mayor interés.

UnDP, Universal device poller, es un colector de información por consultas que utiliza los comandos snmp por el puerto 161 para obtener parámetros en tiempo real del dispositivo gestionado, proporcionando datos estadísticos y reales del estado actual del objeto específico (Paquetes transmitidos, utilización del ancho de banda, voltaje de alimentación, temperatura, etc).

A continuación se presenta el dispositivo bajo prueba:

DISPOSITIVO BAJO PRUEBA	
UBICACIÓN: TORRE DE CONTROL LOS BRASILES	EQUIPO: ROUTER CISCO 2901
	

Se analizarán las notificaciones entrantes provocadas en el dispositivo bajo prueba mostrada en la figura 9 para tratar de identificar los eventos, luego se explicarán algunas de las configuraciones realizadas para las acciones.

TIME OF TRAP	IP ADDRESS	HOSTNAME	COMMUNITY	TRAP TYPE	TRAP DETAILS
24/10/2017 17:25:47			4- #MIB:linkUp		locReason: 13 = up ifType: 13 = 6 ifDescr: 13 = GigabitEthernet0/1/4 ifIndex: 13 = 13 snmpTrapOID = #MIB:linkUp sysUpTime = 218 days 1 hour 10 minutes 20.96 seconds clogHistTimeStamp: 523 = 182942296 clogHistMsgText: 523 = Interface GigabitEthernet0/1/4, changed state to up clogHistMsgName: 523 = UPDOWN clogHistSeverity: 523 = 4 clogHistFacility: 523 = LINK snmpTrapOID = CISCO-SYSLOG-MIB:clogMessageGenerated sysUpTime = 218 days 1 hour 10 minutes 20.96 seconds
24/10/2017 17:25:46			3- CISCO-SYSLOG-MIB:clogMessageGenerated		locReason: 13 = administratively down ifType: 13 = 6 ifDescr: 13 = GigabitEthernet0/1/4 ifIndex: 13 = 13 snmpTrapOID = #MIB:linkDown sysUpTime = 218 days 1 hour 10 minutes 18.96 seconds cmHistoryEventConfigDestination: 16 = 2 cmHistoryEventConfigSource: 16 = 3 cmHistoryEventCommandSource: 16 = commandLine1 snmpTrapOID = CISCO-CONFIG-MAN-MIB:ciscoConfigManEvent sysUpTime = 218 days 1 hour 9 minutes 32.63 seconds cmHistoryEventConfigDestination: 15 = 4 cmHistoryEventConfigSource: 15 = 3 cmHistoryEventCommandSource: 15 = commandLine1 snmpTrapOID = CISCO-CONFIG-MAN-MIB:ciscoConfigManEvent sysUpTime = 218 days 1 hour 8 minutes 26.24 seconds cmHistoryEventConfigDestination: 14 = 2 cmHistoryEventConfigSource: 14 = 3 cmHistoryEventCommandSource: 14 = commandLine1 snmpTrapOID = CISCO-CONFIG-MAN-MIB:ciscoConfigManEvent sysUpTime = 218 days 1 hour 8 minutes 26.24 seconds
24/10/2017 17:25:39			2- #MIB:linkDown		
24/10/2017 17:24:53			1- CISCO-CONFIG-MAN-MIB:ciscoConfigManEvent		
24/10/2017 17:23:47			CISCO-CONFIG-MAN-MIB:ciscoConfigManEvent		
24/10/2017 17:23:43			CISCO-CONFIG-MAN-MIB:ciscoConfigManEvent		

Figura 9: Notificaciones entrantes en Network Performance Monitor

Obsérvese los traps numerados y resaltado en rojo, se describirá cada uno de ellos en orden ascendente empezando con el número 1. Cada segmento de las columnas nos indicara el contenido de la información.

CISCO-CONFIG-MAN-MIB:ciscoConfigManEvent (nombre de la MIB:OID), en este evento se ejecutó el comando #show running configuration el cual muestra la configuración ejecutada en el dispositivo y notifica que se ha registrado dicha consulta

bajo la intervención humana. Esto nos indica que el dispositivo ha sido manipulado y podemos obtener la hora y fecha del evento.

En la primera columna descrita “TIME OF TRAP”.

En la segunda columna, La IP del dispositivo que genero la notificación.

La tercera el nombre en caso de tener un servidor DNS,

En la siguiente muestra la comunidad SNMP a la que pertenece (Aplica para la versión 2 y 2c).

La quinta columna describe el tipo de Trap generado, y por último los detalles del Trap.

2- IF-MIB:linkDown, el nombre del evento se identifica como “Link down”, en la Tabla 3 tenemos una descripción más detallada que se interpreta de la siguiente manera :

Tabla3. Detalles de Trap.

TRAP DETAILS	DESCRIPCION
loclfReason.13 = administratively down	# razón del evento (se fuerza el apagado de la interface)
ifType.13 = 6	# Tipo de interface, definido por la IANA en el módulo mib-2 (ethernetCsmacd(6) -- para todas las interfaces ethernet)
ifDescr.13 = GigabitEthernet0/1/4	# Descripción de la interface involucrada
ifIndex.13 = 13	# Identificación del puerto en el dispositivo
snmpTrapOID = IF-MIB:linkDown	# Nombre de la MIB utilizada
sysUpTime = 218 days 1 hour 10 minutes 25.96 seconds	# Tiempo de operación del sistema desde su ultimo reinicio

Resumiendo, la traducción del informe de la notificación se concluye: en que se reconoce el fallo en uno de los enlaces de comunicación debido al apagado forzado de una de sus interfaces a través de la intervención directa del hombre. La variable ifDescr.13 identifica la interfaz involucrada “GigabitEthernet0/1/4”. OID: 1.3.6.1.6.3.1.1.5.3 es la representación entera en la estructura de la información administrada (SMI) del nombre

de la MIB utilizada. Fecha y hora en la que se generó el evento, 24/10/2017 a las 17:25:39 PM. El agente es el dispositivo bajo prueba quien envía un Trap al gestor tras la ocurrencia del evento, este se identifica con la dirección IP de gestión o con un nombre a través del servidor DNS.

Ya que se ha descrito con detalles la notificación anterior repasaremos brevemente las siguientes:

3- CISCO-SYSLOG-MIB:clogMessageGenerated, evento que indica que se ha generado un mensaje de syslog con una descripción textual e indicando la criticidad del evento como error y resaltado de color rojo. Ver fig. 10

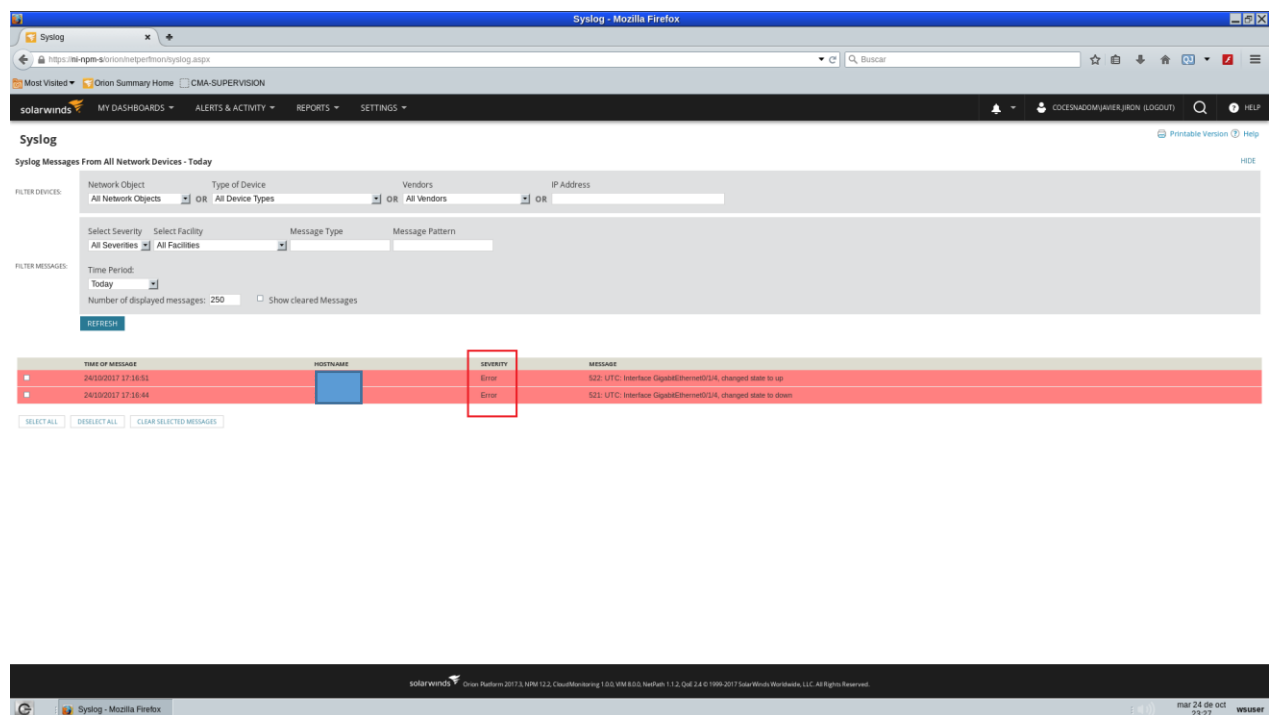


Figura 10. Mensaje Syslog

4- IF-MIB:linkUp, Esta notificación indica que el fallo anterior ha sido superado (Enlace Restablecido) en la interfaz GigabitEthernet0/1/4 con fecha 24/10/2017 a las 17:25:47 PM.

Ya vimos cómo la recepción de notificaciones (Traps) nos ayuda a identificar un problema en la red y la importancia de conocer el estado del dispositivo para una acción correctiva a través del análisis de causa raíz. Ahora en las siguientes figuras, se ilustra como configurar una acción de notificación por correo electrónico a las personas indicadas utilizando la herramienta “trap viewer”.

Para ejemplificar se utiliza la notificación #2 antes descrita. En la figura 11 se abre la herramienta “trap viewer” que se incluye en la aplicación del NPM. Se realiza la búsqueda del trap para crear una regla en la que le configuramos las condiciones que debe cumplir antes de generar una acción específica (en este caso utilizaremos el envío de la notificación por correo electrónico a los destinatarios deseados).

Trap IF-MIB:linkDown, se configuran parámetros generales como el nombre de la regla, la dirección IP del agente, comunidad snmp, etc... que en la mayoría de los casos están por defecto.

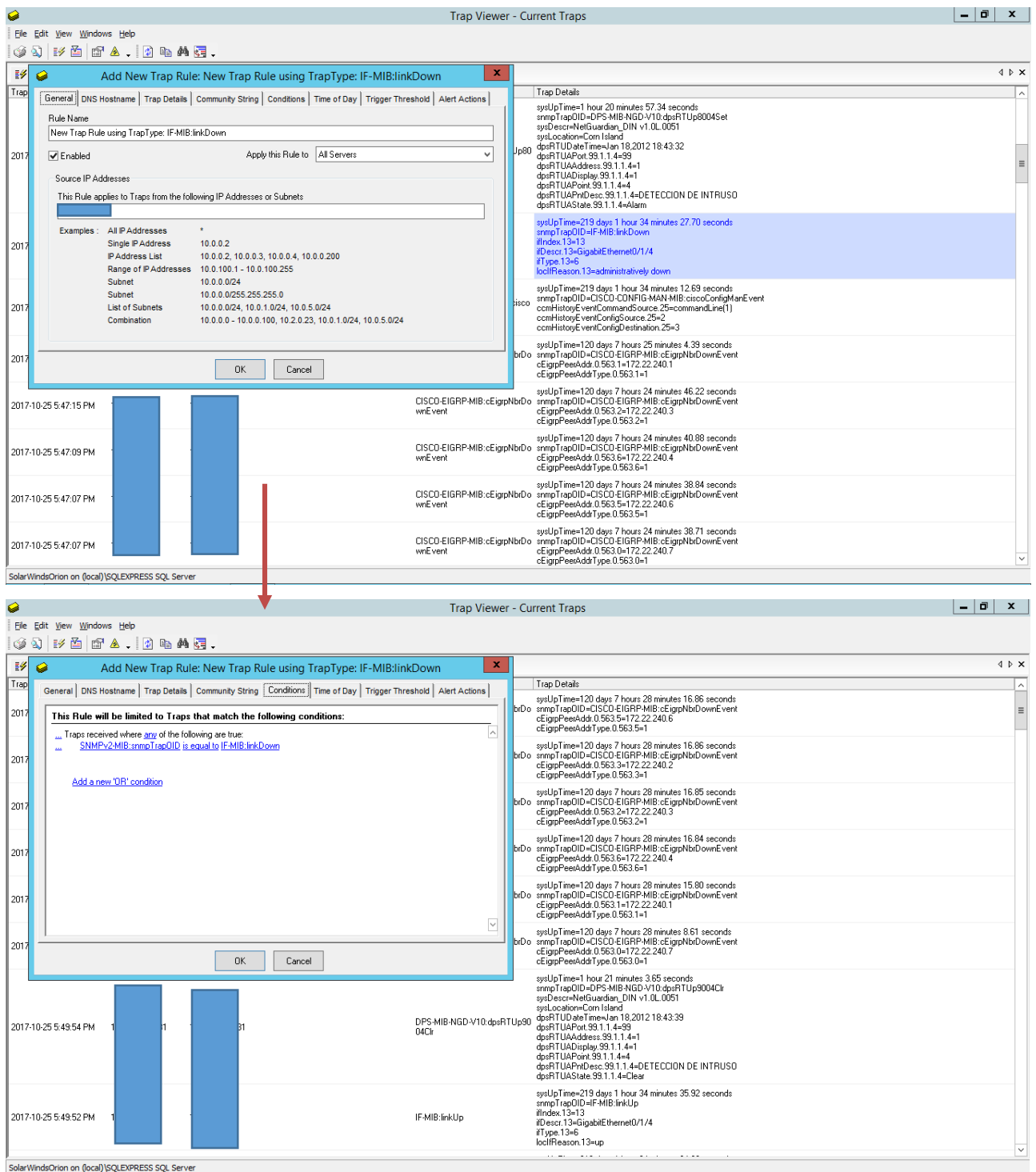


Figura 11. Configuración de los Traps

En la fig. 12 se edita la acción a realizar cuando la condición se cumpla y se enviara un mensaje por correo electrónico a los destinatarios incluidos. El cuerpo del mensaje contendrá el informe Trap y si se desea una descripción personalizada del evento.

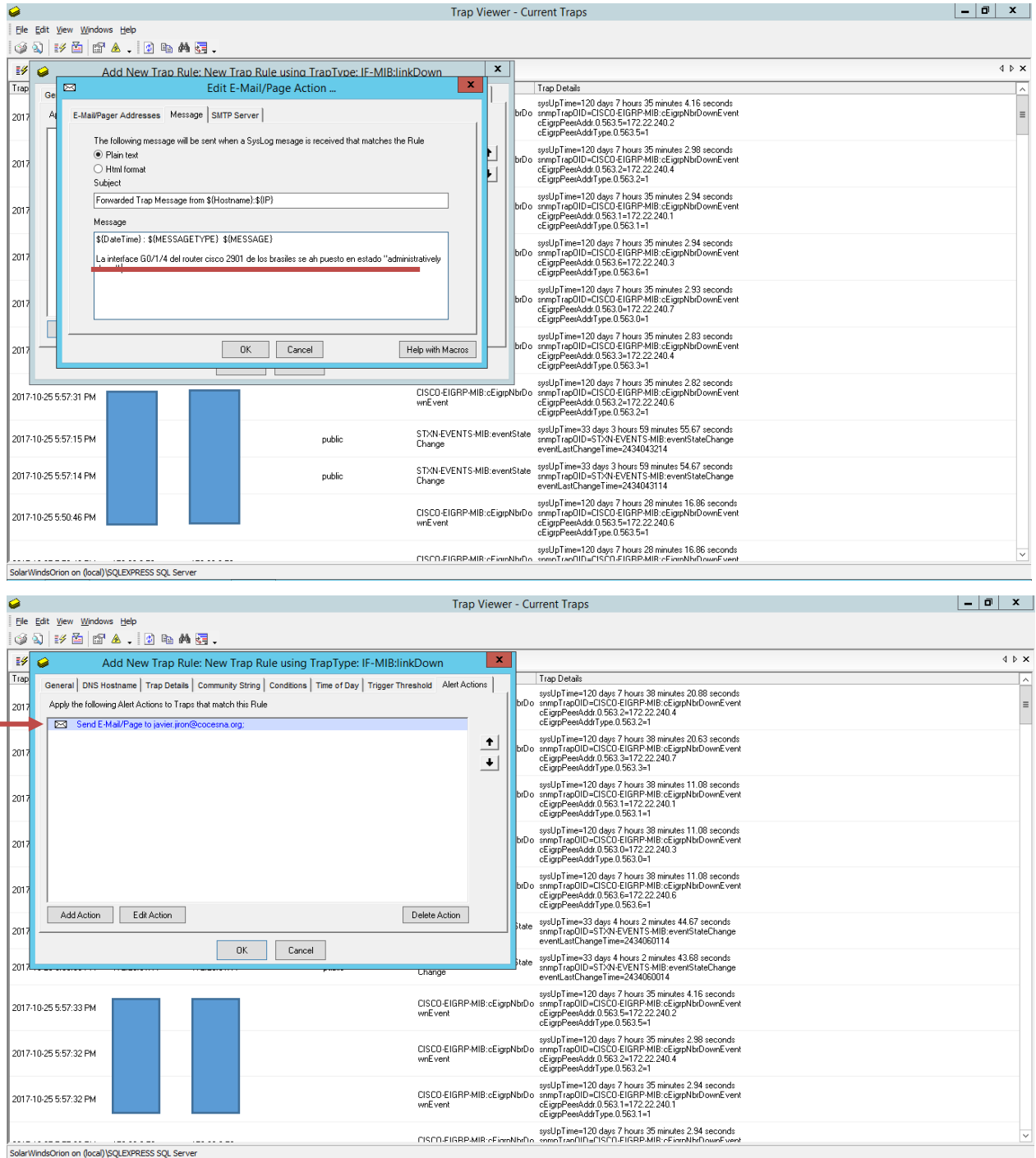


Figura 12. Configuración de los traps Continuación

Se presenta en la fig. 13 el resultado del mensaje enviado a consecuencia de la regla creada para generar una acción.

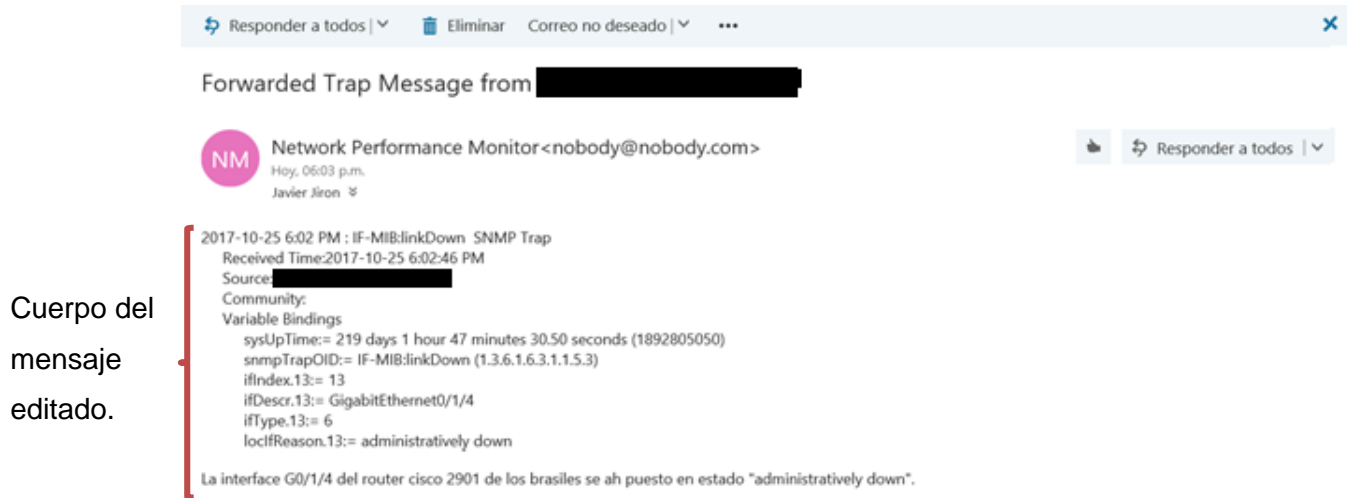



Figura 13. Notificación al correo electrónico.

9.2 PRUEBAS DE OPERATIVIDAD EN DISPOSITIVOS NO SNMP GESTIONADOS ATRAVES DE UN AGENTE PROXY

PRUEBA DE ALARMAS

Para realizar una prueba en el indicador de las alarmas se hizo una acción de control en el cual nos permitirá verificar si las acciones de control se están ejecutando correctamente.

1. En la función de CONTROLS se activa el comando OPR para iniciar el arranque remoto del generador en seguida se pone en estado de ejecutado resaltado en color rojo ver fig. 14.


DPS Telecom
 Network Monitoring Solutions

Localizador Managua

[Home](#) |
 [Upload](#) |
 [Logout \(admin\)](#)

Monitor

Alarms

Controls

Analogs

Sensors

Ping Targets

Modbus Registers

System Alarms

Graph

Stats

Provisioning

Device Access

Controls

Id	Description Display Map	State	Command
1	ARRANQUE REMOTO DE GRUPO ELECTROGENO	Latched	OPR RLS MOM
2	PRUEBA DE RESPALDO DE GRUPO ELECTROGENO	Released	OPR RLS MOM
3		Released	OPR RLS MOM
4		Released	OPR RLS MOM

11/17/2017, 2:39:08 PM

NetGuardian_DIN v1.0L.0007

©2017 DPS Telecom

Figura 14. Arranque Remoto de Grupo Electr geno Activado

- Si nos vamos a la pesta a de alarma podemos observar que se activara la alarma 2. energ a de respaldo, fig. 15; lo cual nos indica que el generador est  operando, sin embargo, este no le suministra la energ a a la carga debido a que la transferencia autom tica no detecta un fallo de la energ a comercial, en ese caso las alarmas que se activaran son; energ a comercial no disponible, energ a de respaldo y carga con energ a de respaldo.

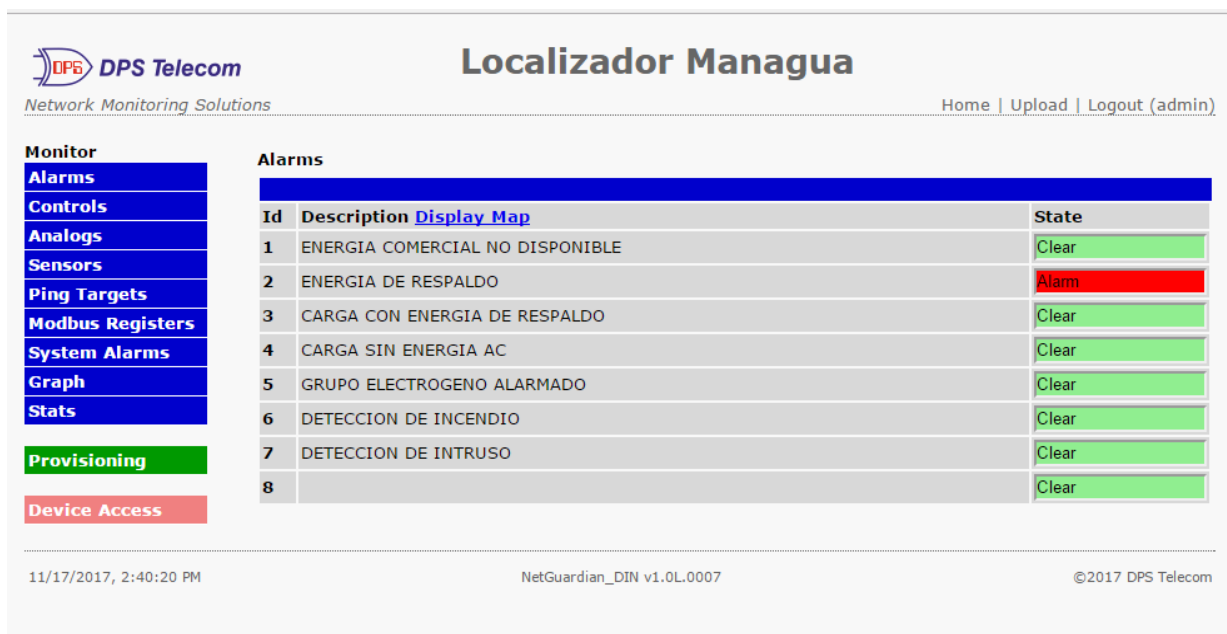


Figura 15. Energía de Respaldo Alarmada

3. Todas estas alarmas serán notificadas al gestor (Solarwinds), además la aplicación de gestión NPM enviara un mensaje de correo electrónico a los técnicos responsables.

En la figura 16 se puede ver la secuencia de la generación de alarmas en solarwinds y como las notificaciones nos pueden ayudar a alertar de un problema potencial en lugares remotos.

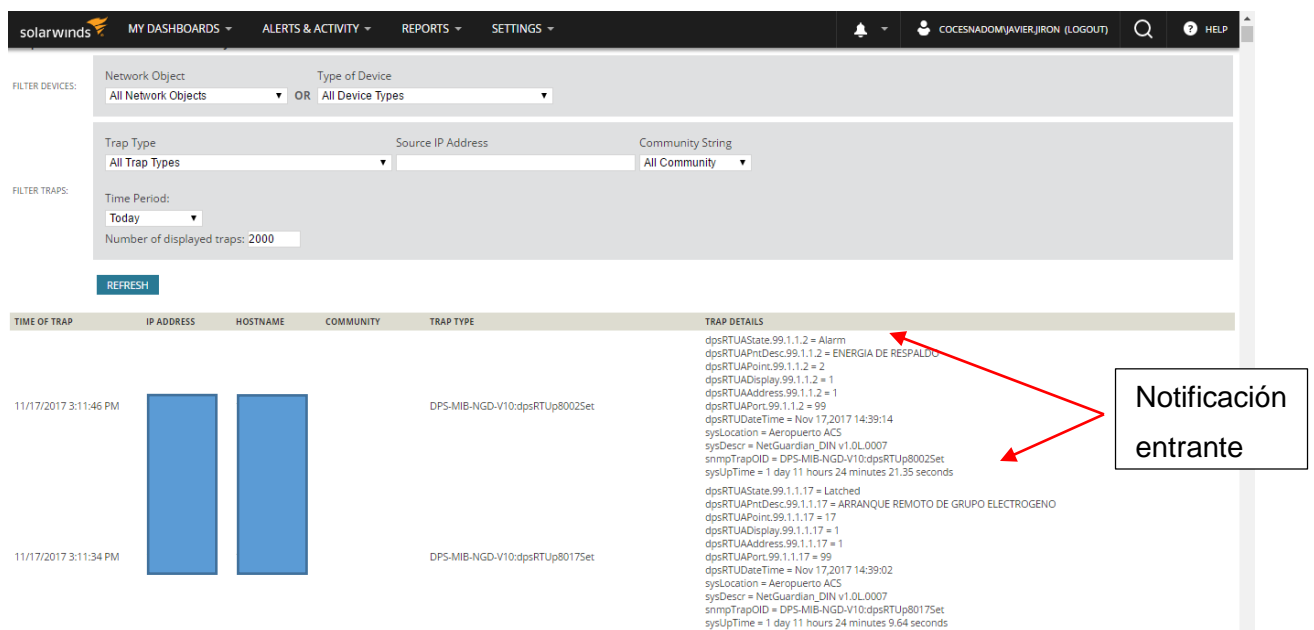


Figura 16. Secuencia de Alarmas en Solarwinds

Obsérvese el anexo 23 el esquema que representa la comunicación SNMP a través de la red los dispositivos que soportan SNMP y los que no soportan SNMP, con la estación administradora.

10. CONCLUSIONES

La implementación del software Solarwinds permite el monitoreo de equipos que soportan o no el protocolo SNMP. Para estos últimos equipos se utilizó un agente proxy o RTU.

Como resultado de la implementación del sistema de monitoreo y control remoto se obtuvieron los siguientes resultados:

- Creación de un banco de datos en donde se recopila la información del funcionamiento del sistema, mostrando fallas, incidentes, tiempo que estuvieron fuera de servicio, etc...
- En caso de algún fallo en los dispositivos gestionados existe una acción según sea la configuración establecida.
- Verifica los parámetros de funcionamiento de los componentes del sistema, en caso de anomalías, manda un correo vía e-mail a los ingenieros encargados del sistema para su debida corrección.
- Acciones de control para la realización de pruebas de operatividad de los dispositivos de comunicación.

11. RECOMENDACIONES

A lo largo del desarrollo del trabajo monográfico se identificaron las siguientes recomendaciones:

- Utilizar estadísticas generadas por Solarwinds para la presentación de auditorias
- Involucrar a todo el personal de COCESNA para un mejor aprovechamiento de esta herramienta de monitoreo.
- Solicitar al momento de compra de nuevos sistemas que estos puedan ser gestionados a través de la red para su integración en Solarwinds.

12. BIBLIOGRAFIA

- [1] SNMP PROTOCOL, Accessed August 2017. [Online]. Available: <http://infotelecommil.webcindario.com/librostelecom/SNMP.pdf>
- [2] H. Jones, S. Rosales, "Implementación de un Agente SNMP", Memoria de título, Lic. en Electrónica, Depto. De Ing. Eléctrica, Universidad Autónoma Metropolitana, itzalapa, México, 1995.
- [3] Douglas R. Mauro and Kevin J. Schmidt, Essential SNMP, Second Edition, United States of America, O'Reilly Media 2005.
- [4] N Botero, "modelo de gestión de seguridad con soporte a SNMP", Memoria de título, Ing. en Sistemas, Facultad de Ingeniería, Pontificia Universidad Javeriana, Bogotá, Colombia, Junio 2005.
- [5] j.Case,M. Fedor, M. Schoffstall, J. Davin, « A Simple Network Management Protocol (SNMP) ,» *RFC 1157, 1990.*
- [6] R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser
« Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP),» *RFC 3416, 2002.*
- [7] R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser
, «Transport Mappings for the Simple Network Management Protocol (SNA Simple Network Management Protocol (SNMP),» *RFC 3417, 2002.*
- [8] R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser
, «Management Informatio Base(MIB) for the Simple Network Management Protocol (SNMP),» *RFC 3418, 2002.*

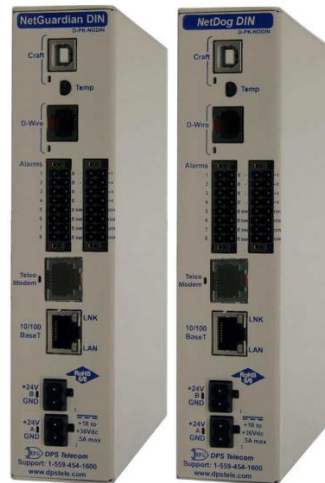
- [9] D. Levi, P. Meyer, B. Stewart, «SNMPv3 Applications» *RFC 2273*, 1998.
- [10] U. Blumenthal, B. Wijnen, , «user-based security model (USM) for version 3 of the simple network Management protocol (SNMPv3)» *RFC 2274*, 1998
- [11] B. Wijnen, R. Presuhn, K. McCloghrie, , «view-based access control model (VACM) for the simple network Management protocol (SNMP)» *RFC 2275*, 1998
- [12] SolarWinds® Orion® Network Performance Monitor Quick Start Guide version 10.5, 6.04.2013
- [13] (2017) Cocesna. Accessed November 2017. [Online]. Available: <http://cocesna.org/acna/>
- [14] (2017) Cocesna. Accessed November 2017. [Online]. Available: <http://cocesna.org/acsa/>
- [15] Net guardian din/NetDog Din user manual, DPS Telecom, 2017.
- [16] Orion Application Performance Monitor Evaluation Guide, Version 2.5, 3.3.2009
- [17] Wendell Odom, Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide, Indianapolis, USA, Pearson Education 2013.

13. ANEXOS

NetGuardian DIN/ NetDog DIN

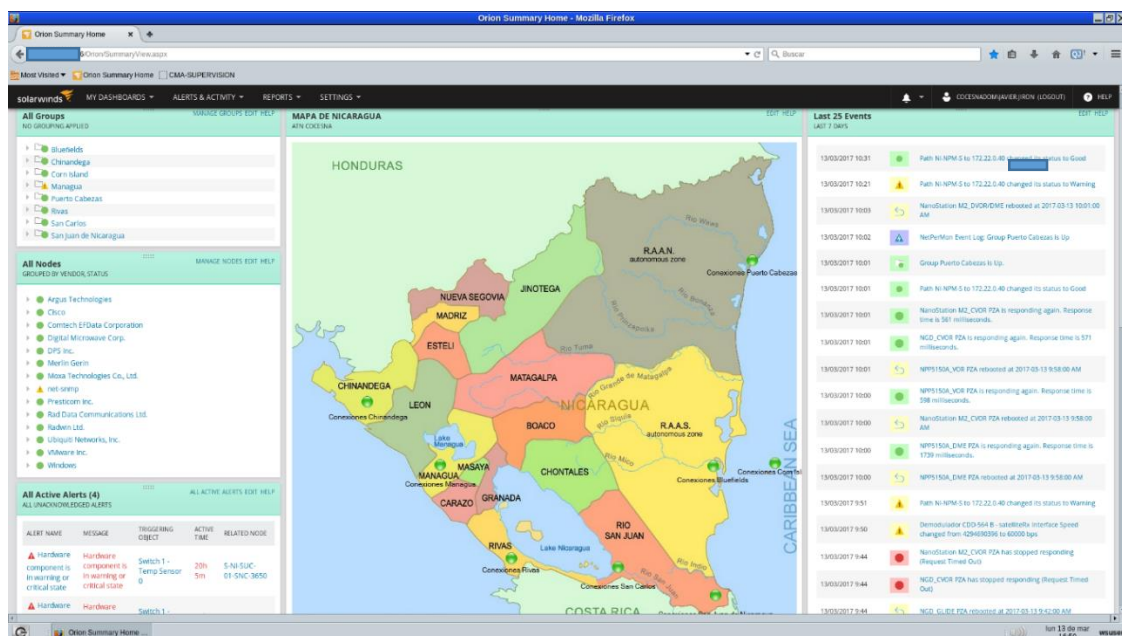
USER MANUAL

D-PK-NGDIN



Visit our website at www.dpstelecom.com for the latest PDF manual and FAQs.

Anexo 1. RTU, modelo NetGuardian Din, Fabricante DPS Telecom



Anexo 2. Mapa de Nicaragua personalizado.

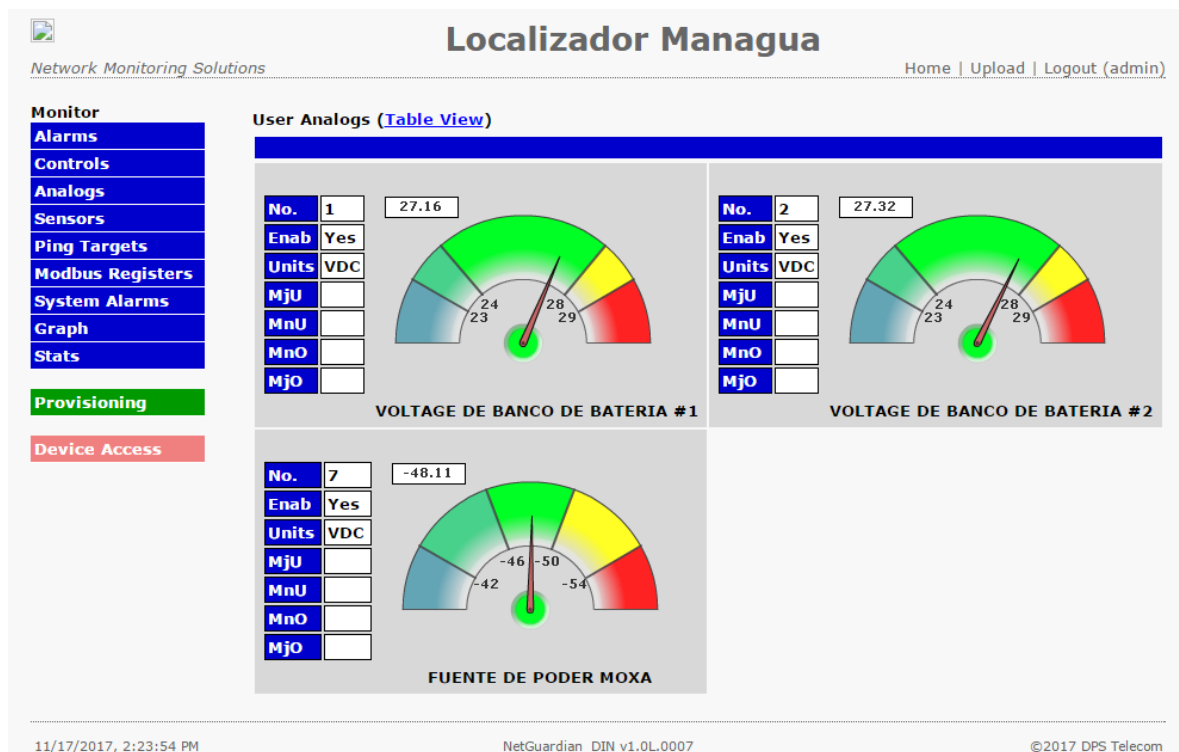


Anexo 3. Panel de alarmas de las variables del entorno conformado por Switch POE para la conectividad de red TCP/IP al Agente Proxy y un convertidor Serie/Ethernet para la administración del sistema ILS.

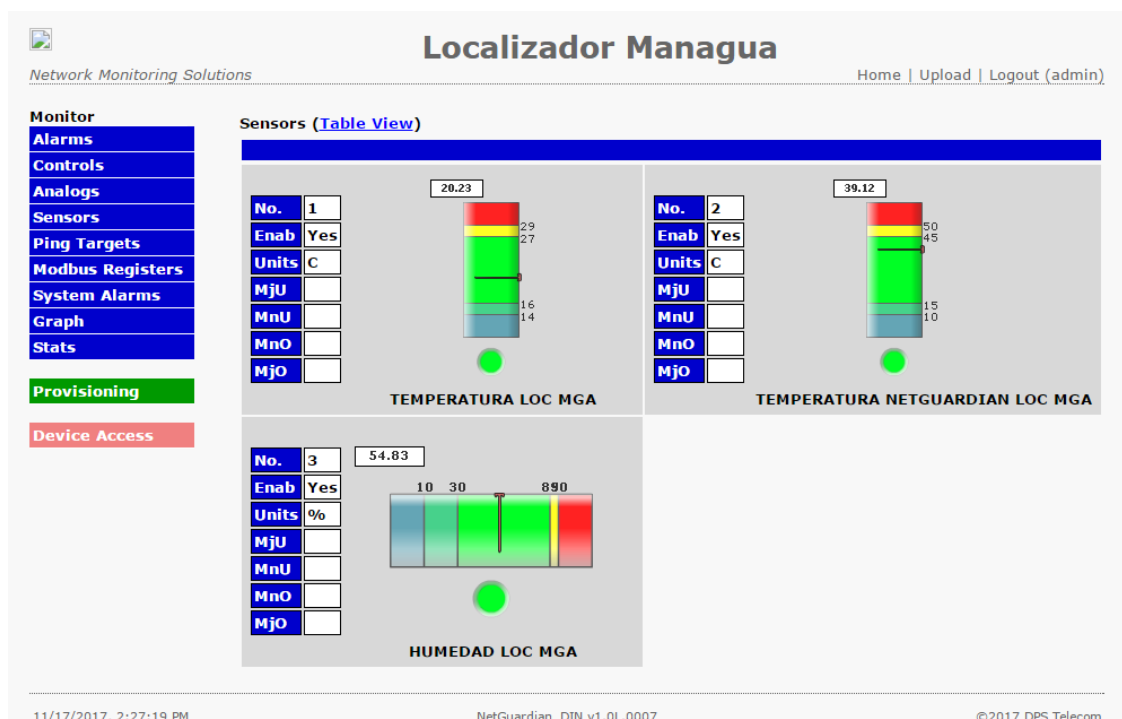
Especificaciones de Net guardian Din	
Protocolos:	SNMPv1, SNMPv2c, SNMPv3, DCPx, TELNET, HTTP, HTTPS, Email, TRIP
Dimensiones	2.1" H x 7.250" W x 5.150" D
Peso	1.13 lbs (.513 kg)

Interface Visual:	7 LEDs en panel frontal
Temperature de Operación	32° - 140° F (0° - 60° C)
Opcion de Temperatura industrial:	-22° to 158° F (-30° to 70° C)
Compatibilidad con Windows :	XP, Vista, 7 (32 o 64 bit)
Sensores:	Hasta 15 sensores

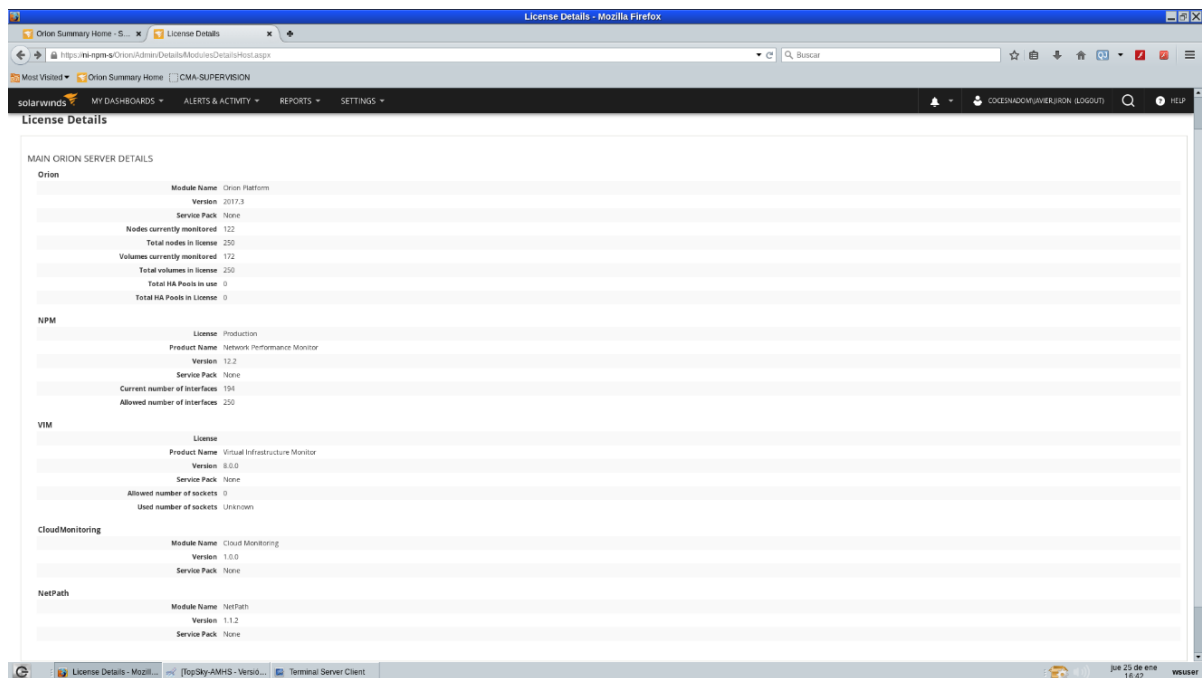
Anexo 4. Especificaciones de RTU NetGuardian Din



Anexo 5. Visualización de variables análogas monitoreadas en el web server de NetGuardian Din.



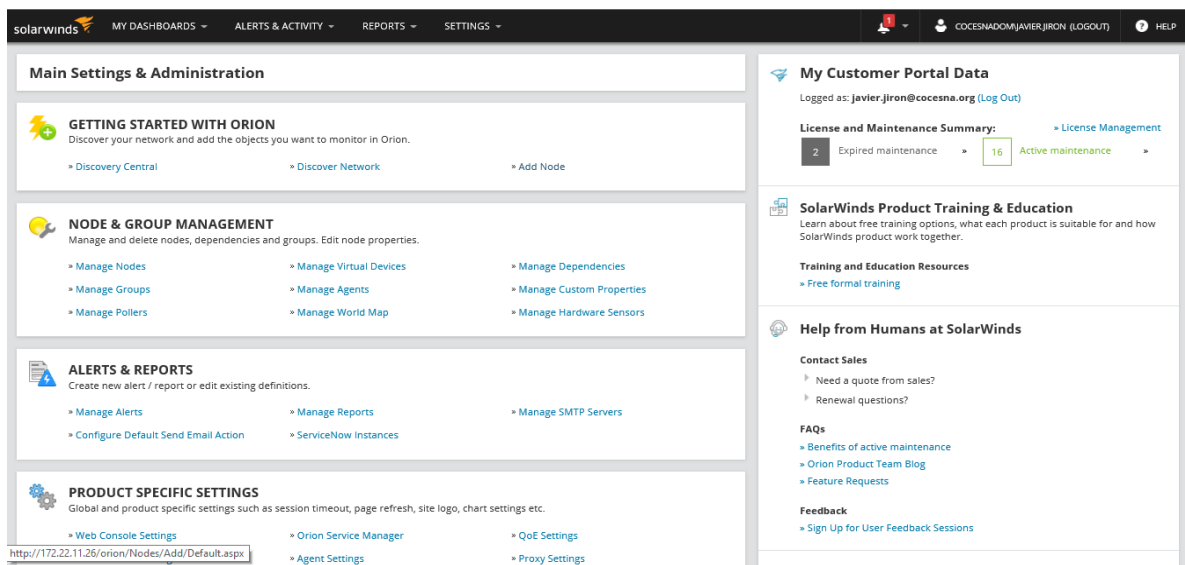
Anexo 6. Visualización de sensores monitoreados en el web server de NetGuardian Din.



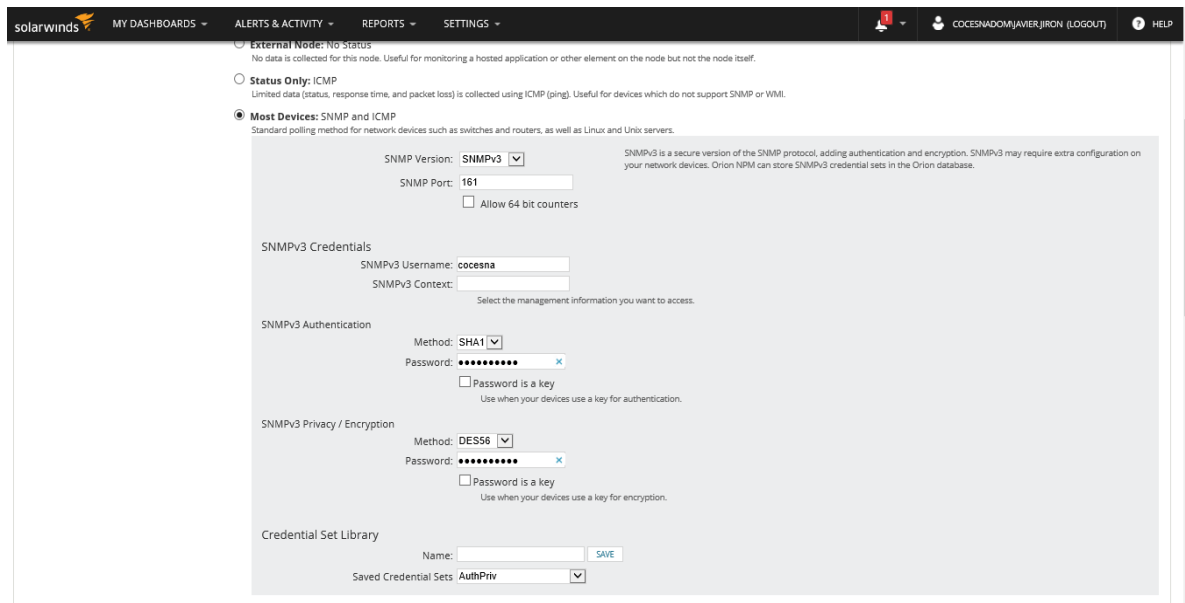
Anexo 7. Detalle de Licencia adquirida por COCESNA

NAME	ROUTER CISCO	Define la versión del protocolo que se utiliza en el dispositivo.
Polling IP Address	xxx.xxx.xxx.xxx	Dirección IPv4 o IPv6 del dispositivo.
SNMP Versión	SNMPv3	Define la versión del protocolo que se utiliza en el dispositivo.
SNMP Port	161	Valor numérico del puerto de red que utiliza el agente para el envío de las notificaciones (Traps).
SNMPv3 Username	Cocesna	Nombre de usuario para la gestión.
SNMPv3 Authentication Method	NONE SHA1 MD5	Especifica el algoritmo de encriptación a utilizar para la autenticación.
SNMPv3 Privacy / Encryption Method	NONE DES56 AES128 AES192 AES256	Define el método de cifrado de la información.
Polling	Node Status Polling. Collect Statistics. Poll for Topology Data.	Definición de los intervalos de tiempos para la recolección de información.
Custom Properties	City Comments Department	Descripción del Objeto gestionado.

Anexo 8. Datos mas relevantes para realizar configuración SNMP



Anexo 9. Pestana de Configuración para agregar un nuevo nodo a Solarwinds.



Anexo 10. Introduciendo el Nodo a Solarwinds

solarwinds MY DASHBOARDS ALERTS & ACTIVITY REPORTS SETTINGS

Method: None
 Password:
☐ Password is a key
 Use when your devices use a key for encryption.

Credential Set Library
 Name: SAVE
 Saved Credential Sets:

TEST Test Successful

☐ Windows Servers: WMI and ICMP
 Recommended agentless polling method for Windows servers.

☐ Windows & Linux Servers: Agent
 Optional agent useful for monitoring Windows & Linux hosts in remote or distributed environments, such as the cloud. Credentials are needed only for installing the agent. The agent does not need to be installed on the server already.
[What is an agent?](#)

☐ Meraki Wireless: API
 API based polling for Meraki wireless gear.

Additional Monitoring Options:
☐ UCS manager credentials
 If the node hosts an UCS manager, check to enter credentials

☐ Poll for VMware
 The VMware API is used to collect host information. SNMP is used to collect statistics for both hosts and guest nodes.

☐ Poll for FS iControl
 The FS iControl API is used to collect health monitor statistics.

NEXT CANCEL

solarwinds Orion Platform 2017.1, NPM 12.1, VM 7.0.0, NetPath 1.1.0, QoS 2.3 © 1999-2017 SolarWinds Worldwide, LLC. All Rights Reserved.

Anexo 11. Introduciendo el nodo a Solarwinds.

solarwinds MY DASHBOARDS ALERTS & ACTIVITY REPORTS SETTINGS

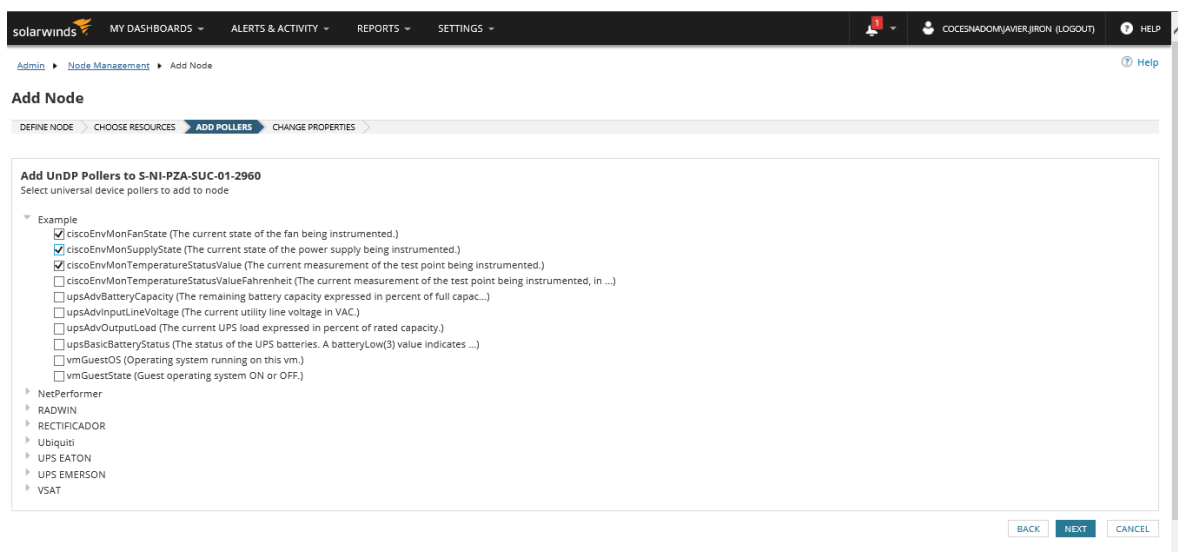
DEFINE NODE CHOOSE RESOURCES ADD POLLERS CHANGE PROPERTIES

Choose Resource to monitor on S-NI-PZA-SUC-01-2960
 Select the resources and statistics to monitor. The select menu provides shortcuts for selections

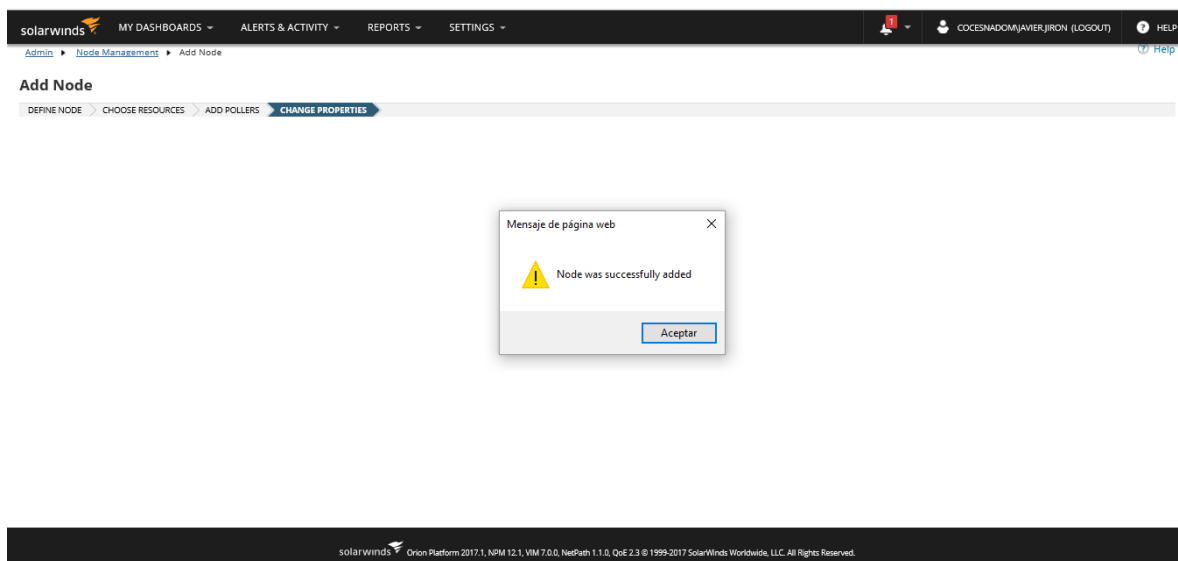
Select: ☒ ALL ☐ NONE ☒ ALL VOLUMES ☒ ALL INTERFACES ☒ ALL ACTIVE INTERFACES ☐ NO INTERFACE STATISTICS

☒ Hardware Health Sensors
☒ Routing
☒ Routing table
☒ CPU & Memory
☒ Status & Response Time
☒ ICMP (Ping) - Fastest
☐ SNMP
☒ Topology: Layer 2
☒ Topology: Layer 3
☒ VLAN
☒ EnergyWise
☐ Vlan1 - V11
☒ Vlan300 - RED VSAT
☐ StackPort1
☐ StackSub-Sct1-1
☐ StackSub-Sct1-2
☐ GigabitEthernet1/0/1 - Gi1/0/1
☐ GigabitEthernet1/0/2 - Gi1/0/2
☐ GigabitEthernet1/0/3 - Gi1/0/3
☐ GigabitEthernet1/0/4 - Gi1/0/4
☐ GigabitEthernet1/0/5 - Gi1/0/5
☐ GigabitEthernet1/0/6 - Gi1/0/6
☐ GigabitEthernet1/0/7 - Gi1/0/7
☐ GigabitEthernet1/0/8 - Gi1/0/8
☐ GigabitEthernet1/0/9 - Gi1/0/9
☐ GigabitEthernet1/0/10 - Gi1/0/10
☐ GigabitEthernet1/0/11 - Gi1/0/11

Anexo 12. Selección de parámetros de interés.



Anexo 13. Selección de parámetros de interés.



Anexo 14. Nodo finalmente agregado

solarwinds MY DASHBOARDS - ALERTS & ACTIVITY - REPORTS - SETTINGS -

COCESNADOMJAWERJIRON (LOGOUT) HELP

Manage Groups

Groups may contain any number of Orion objects. You may alert and report on groups. Groups also have summary and detail views.

Group by: Parent (Groups) View mode: All Groups ADD NEW GROUP EDIT PROPERTIES ADD & REMOVE OBJECTS VIEW DYNAMIC QUERY RESULTS DELETE

Name	Object type	Description
Bluefields	Group	Nodos ubicados en la R.A.A.S.
Chinandega	Group	Nodos ubicados en el departamento de chinandega
Corn Island	Group	Nodos ubicados en la isla del atlantico
Managua	Group	Nodos ubicados en el departamento de Managua
Puerto Cabezas	Group	Nodos ubicados en la R.A.A.N.
Plus 5 more objects (Only first 20 are displayed)		
R-NI-TWRPZA-SUC-01	Node	
R-NI-PZA-SUC-01-2921	Node	
PZA_VOR NPP5150A	Node	
PZA_TWR Servidor ATIS Maestro	Node	
PZA_TWR Servidor ATIS Esclavo	Node	
PZA_TWR Rocket M2	Node	
PZA_TWR Estacion ATIS	Node	
PZA_NETPERFORMER	Node	
PZA_NetGuardianM16	Node	

Page 1 of 1 Displaying items 1 - 8 of 8

solarwinds Orion Platform 2017.1, NPM 12.1, VM 7.0.0, NetPath 1.1.0, QoS 2.3 © 1999-2017 SolarWinds Worldwide, LLC. All Rights Reserved.

Anexo 15. Verificando que el nodo fue agregado.

solarwinds MY DASHBOARDS - ALERTS & ACTIVITY - REPORTS - SETTINGS -

COCESNADOMJAWERJIRON (LOGOUT) HELP

Admin Manage Groups Add & Remove Orion Objects

Add & Remove Orion Objects - Puerto Cabezas

Add Orion objects to your group by dragging them from the left to the right panel or select multiple objects using checkboxes and use "Add Objects to Group" button. Dynamic query objects can be used to populate groups dynamically.

AVAILABLE OBJECTS

SHOW ONLY: Nodes

GROUP BY: Vendor

SEARCH FOR:

SELECT ALL SELECT NONE

- LMNG_VSAT
- PCH_CORE
- PCH_CORE
- R-NI-BLU-SUC-01-2921
- R-NI-CIS-SUC-01-2921
- R-NI-SNC-SUC-01-2921
- R-NI-TWRBLU-SUC-01
- SJN_CORE
- S-NI-BLU-ACC-01-3650
- S-NI-MGA-TWR-01-2960
- S-NI-SUC-01-SNC-3650
- SW-NI-CIS-SUC-01-3650
- Comtech EFData Corporation (13)
- Digital Microwave Corp. (1)
- DPS Inc. (5)
- Emerson Computer Power (1)

ADD TO GROUP REMOVE

PUERTO CABEZAS

ADD DYNAMIC QUERY EDIT DYNAMIC QUERY VIEW DYNAMIC QUERY RESULTS SELECT ALL SELECT NONE

- PZA_Modem CDM-570 A
- PZA_Modem CDM-570 B
- PZA_NetGuardianM16
- PZA_NETPERFORMER
- PZA_RADAR WL-1000 A
- PZA_RADAR WL-1000 B
- PZA_TWR Estacion ATIS
- PZA_TWR Rocket M2
- PZA_TWR Servidor ATIS Esclavo
- PZA_TWR Servidor ATIS Maestro
- PZA_TWR WL-1000 A
- PZA_TWR WL-1000 B
- PZA_VOR NPP5150A
- R-NI-PZA-SUC-01-2921
- R-NI-TWRPZA-SUC-01
- S-NI-PZA-SUC-01-2960

SUBMIT CANCEL

Anexo 16. El nodo agregado junto a los demás nodos en el departamento de Puerto Cabezas.



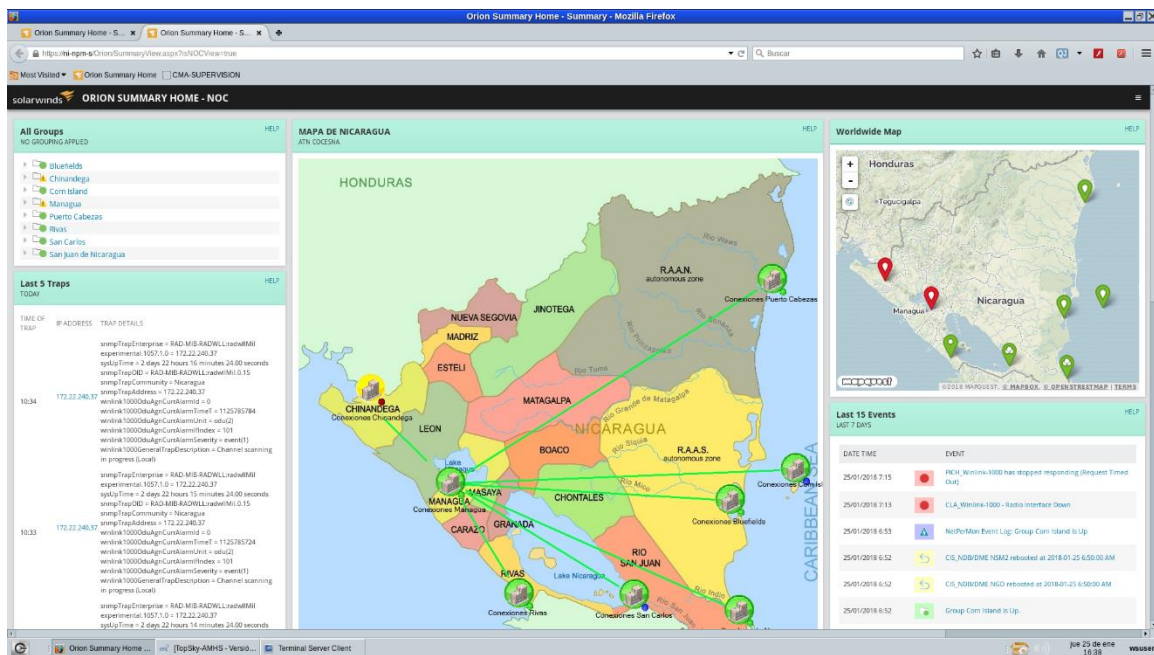
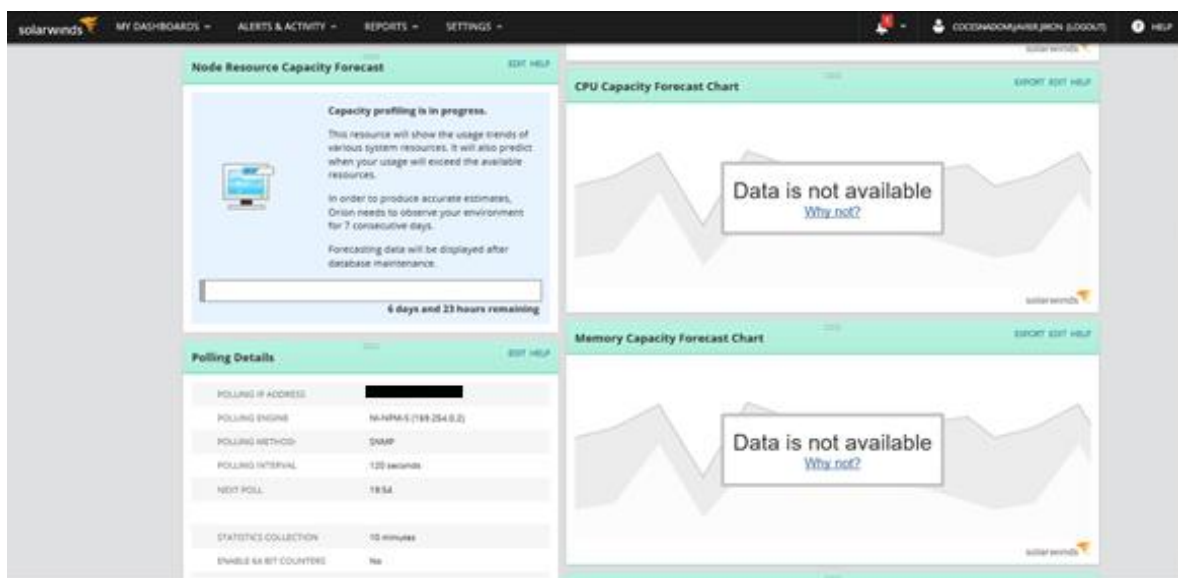
Anexo 17. Nodos de puerto Cabezas

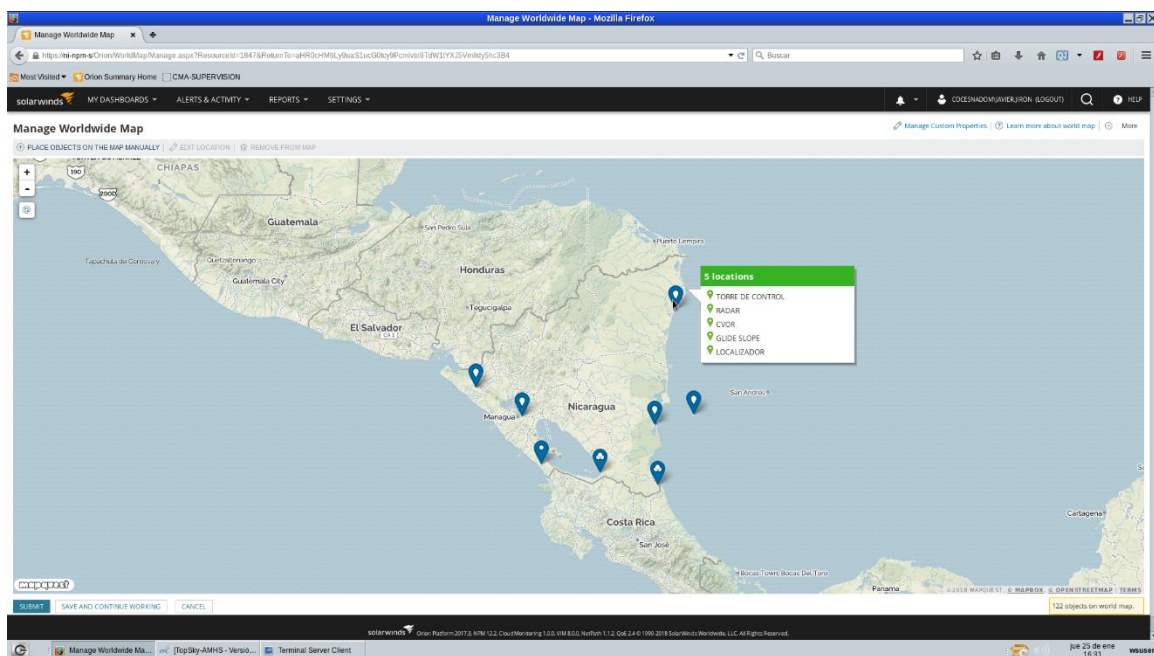
The screenshot shows the 'Edit Resource: Top CPUs by Percent Load' configuration page in the SolarWinds Orion Platform. The page includes the following fields and options:

- Title:** Top CPUs by Percent Load
- Subtitle:**
- Calculated series:** ☐ Show the sum of all data series
- Time periods:**
 - Default zoom range: Today
 - Amount of historical data to load: Last 1 Day
 - Sample interval: Every 30 minutes
- Advanced:** ☐ (checked)
- SUBMIT** button

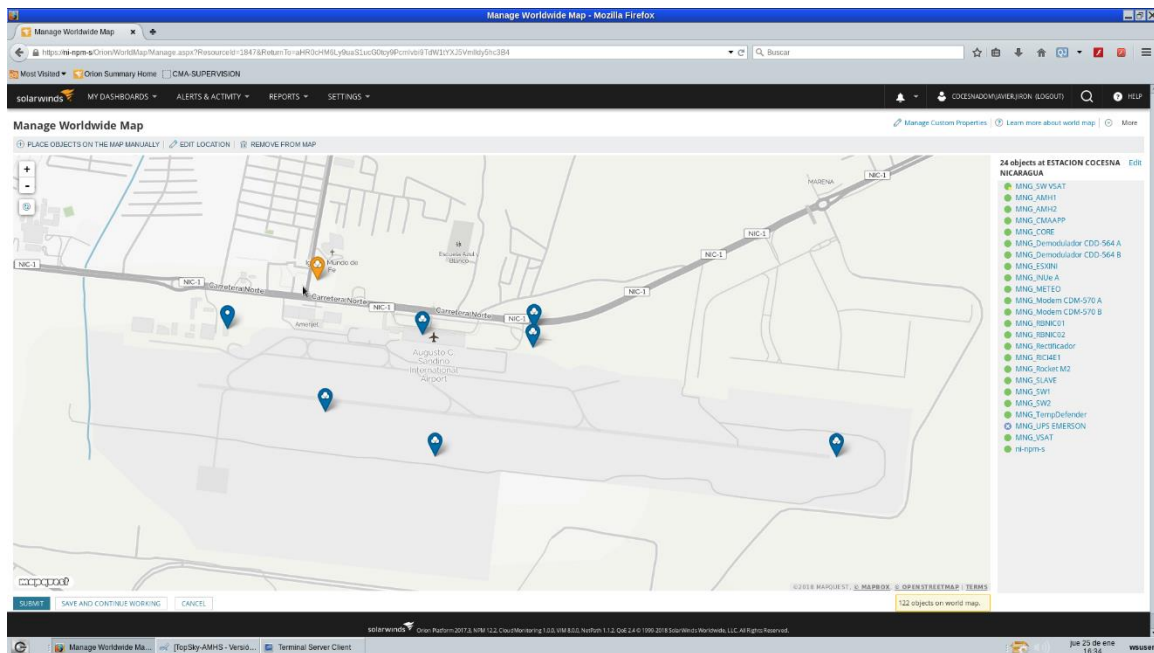
At the bottom of the page, the footer text reads: 'solarwinds Orion Platform 2017.1, NPM 12.1, VM 7.0.0, NetPath 1.1.0, QoS 2.3.9 1999-2017 SolarWinds Worldwide, LLC. All Rights Reserved.'

Anexo 18. Edición de tiempos de polleo en el nodo de Puerto Cabezas.

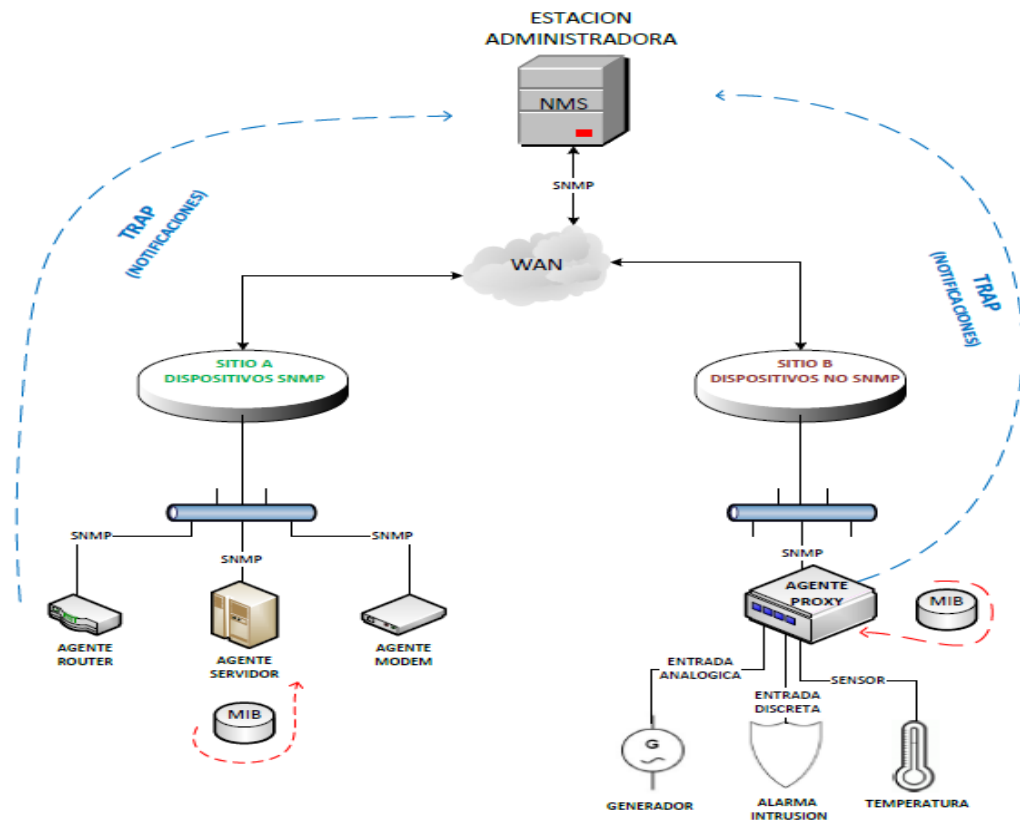




Anexo 21. Vista de los sitios instalados en Nicaragua.



Anexo 22. Visualización de los distintos sistemas instalados en el Aeropuerto Augusto Cesar Sandino.



Anexo 23. Esquema que representa la comunicación SNMP con la estación administradora.